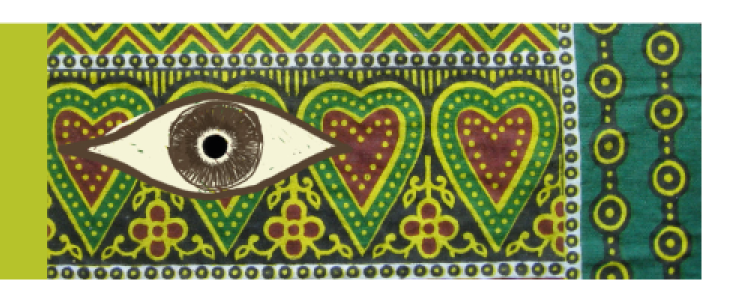
Manual de seguridad





http://es.security.ngoinabox.org

Guía Paso a Paso

Esta Guía Paso a Paso está diseñada para explicar los temas que debes entender con el fin de salvaguardar tu propia seguridad digital. Esta busca identificar y describir los riesgos que enfrentas y ayudarte a tomar decisiones informadas de cómo reducir, de la mejor manera, dichos riesgos. En este extremo, responde a ocho preguntas generales relacionadas a seguridad básica, protección de datos y privacidad de las comunicaciones.

Al inicio de cada capítulo, encontrarás un contexto poblado de personajes ficticios que reaparecerán en breves diálogos a lo largo del capítulo con el fin de ilustrarte sobre ciertos aspectos y respuestas a preguntas comunes. También encontrarás una corta lista de lecciones especificas que pueden ser aprendidas a partir de la lectura del capítulo. Es una buena idea darle un vistazo a esta lista antes de que empieces a leer. A medida que te desplazas en el capitulo, encontraras varios términos técnicos que se enlazan con definiciones en un glosario que se halla al final de la guía. También encontraras referencias al programa específico tratado en el paquete de las Guías Prácticas.

Cualquier capitulo o guía independiente en este paquete puede leerse individualmente, darle formato en tu navegador para una fácil impresión, o compartirlo electrónicamente. Sin embargo, aprovecharás de mejor manera la Caja de Seguridad si sigues los enlaces pertinentes y las referencias que están esparcidas a lo largo de la guía y de las guías de los programas. Si tienes una copia física de la Guía Paso a Paso, debes mantenerla frente a ti mientras trabajas con las Guías Prácticas. También debes recordar el finalizar la lectura del capitulo de la Guía Paso a Paso que cubre una herramienta específica antes de confiar en dicha herramienta para que proteja tu seguridad digital.

En la medida de lo posible, debes leer los capítulos de la Guía Paso a Paso en orden. La seguridad es un proceso, y no es coherente intentar defenderte de una amenaza avanzada a la privacidad de tus comunicaciones, por ejemplo, si no has garantizado que tu computadora está libre de virus y de otros software malintencionados (malware). En muchos casos, esto puede parecerse a cerrar tu puerta una vez que el ladrón está ya en tu casa. Esto no quiere decir que alguno de los ocho temas sea más importante que cualquier otro, sino que simplemente los últimos capítulos hacen algunas suposiciones sobre lo que ya sabes y sobre el estado de la computadora en la cual instalarás el programa.

Claro que existen muchas buenas razones por las que tú quisieras recorrer estos capítulos sin secuencia. Puede que necesites consejos de cómo crear un respaldo a tus archivos más importantes antes de empezar a instalar las herramientas descritas en la primera Guía Práctica. Puede ser que afrontes una amenaza urgente a tu privacidad que justifica que aprendas como proteger tu información sensible en tu computadora, lo cual esta cubierto en el *Capítulo 4*, lo más rápido posible. Talvez estás trabajando en un café Internet, en una computadora cuya seguridad no es tu responsabilidad y desde la cual no pretendes acceder a alguna información sensible. Si deseas utilizar esta computadora para visitar un sitio web que esta bloqueado en tu país, no existe nada que te impida saltar hasta el *Capítulo 8. Mantenerse en el anonimato y evadir la censura en Internet*.

1. Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers)

Sin importar cuales sean tus más amplios objetivos, el mantener tu computadora libre de problemas es un primer paso indispensable en la senda de una mejor seguridad. Por ello, antes de empezar a preocuparte demasiado - por ejemplo, acerca de contraseñas sólidas - comunicación privada y borrado seguro, necesitas garantizar que tu computadora no sea vulnerable a los *piratas informáticos (hackers)* o no esté plagada de *software malicioso (malware)*, tales como virus y software espía (spyware). De lo contrario, es imposible garantizar la efectividad de cualquier otra precaución de seguridad que pudieras tomar. Después de todo, no tiene sentido cerrar la puerta si el ladrón ya se encuentra en nuestras escaleras, y tampoco es bueno buscar en las escaleras si dejas la puerta completamente abierta.

De la misma manera, este capítulo explica como mantener tu software y utilizar herramientas como el *Avast*, *Spybot* y *Comodo Firewall* para proteger tu computadora de peligros permanentes de infección de *software malicioso (malware)* y ataques de *piratas informáticos (hackers)* . Aunque las herramientas recomendadas en este capítulo son para Windows - que es el sistema operativo más vulnerable a estas amenazas - los usuarios de *GNU/Linux* y Apple OS X también se hallan en riesgo y deben seguir las tácticas referidas a continuación.

Contexto

Assani es un activista de derechos humanos en un país africano francófono. Sus dos hijos adolescentes, Salima y Muhindo, se han ofrecido a ayudarle con algo de trabajo informático de rutina que le solicitaron a él. Después de ver el estado de su computadora, ellos se han ofrecido a enseñarle lo fundamental en cuanto a mantenerla libre de problemas y funcionando plenamente. A Assani también le entusiasma la idea de utilizar Software Libre y de Código Abierto (FOSS) , pero no está seguro si ello será más o menos seguro, de modo que también les pide su consejo.

¿Qué aprenderás en este capítulo?

- Unas cuantas amenazas específicas que plantea el *software malicioso (malware)* a la privacidad e integridad de tu información, la estabilidad de tu computadora y la confiabilidad de otras herramientas de seguridad
- Cómo puedes utilizar varias herramientas recomendadas para ayudar a protegerte de estas amenazas
- Cómo mantener tu computadora segura actualizando tu software frecuentemente
- Porqué debes utilizar herramientas de *software gratuito (freeware)*, para evitar los peligros asociados con licencias expiradas o software pirata, y populares herramientas de *Software Libre y de Código Abierto (FOSS)*, cuando sea posible para mejorar tu seguridad

Virus

Existen muchas maneras distintas de clasificar los virus, y cada una de estas viene acompañada de su propia colección de categorías con nombres pintorescos. Gusanos, macrovirus, troyanos y puertas traseras (backdoors) son algunos de los ejemplos más conocidos. Muchos de estos virus se extienden en Internet, utilizando el correo electrónico, páginas web maliciosas u otros medios para infectar computadoras no protegidas. Otros se propagan a través de medios extraíbles, particularmente a través de dispositivos USB y de discos duros externos que permiten a los usuarios escribir y leer información. Los virus pueden destruir, dañar o infectar la información en tu computadora, incluyendo datos en discos externos. Estos también pueden tomar control de tu computadora y utilizarla para atacar a otras. Afortunadamente existen muchas herramientas antivirus que puedes utilizar para protegerte y proteger a aquellos con los cuales intercambias información digital.

Software Antivirus

Existe un excelente programa antivirus que además es *software gratuito (freeware)* para Windows llamado *Avast*, el cual es fácil de utilizar, se actualiza de manera regular y es respetado por los expertos en programas antivirus. Este requiere que te registres una vez cada 14 meses, pero el registro, las actualizaciones y el programa son gratuitos.

Clam Win es una alternativa de *Software Libre y de Código Abierto (FOSS)* al *Avast* y de varios conocidos programas comerciales antivirus. Aunque carece de ciertas características que son importantes para un programa antivirus básico, Clam Win tiene la ventaja que puede ser ejecutado desde una memoria extraíble USB con el fin de escanear una computadora en la cual no se te permite instalar software. Esto es extremadamente útil cuando no tienes otra opción más que utilizar una computadora pública o los cafés Internet para realizar trabajo sensible.

Consejos para utilizar software antivirus de manera eficaz

- No ejecutes dos programas antivirus al mismo tiempo, pues ello podría causar que tu computadora funcione de manera extremadamente lenta o que se cuelgue. Desinstala uno antes de instalar otro.
- Asegúrate que tu programa antivirus te permita recibir actualizaciones. Como muchas de las herramientas comerciales que vienen preinstaladas en las computadoras nuevas, en algún punto se debe proceder a registrarlas (y pagar por ellas) o estas dejarán de recibir actualizaciones. Todo el software que se recomienda aquí permite actualizaciones libres de cargo.

- Cerciórate que tu software antivirus se actualice automáticamente de manera regular. Los nuevos virus se crean y propagán a diario, y tu computadora pronto se verá vulnerable si no estás al tanto de nuevas definiciones de virus. *Avast* automáticamente buscará actualizaciones cuando te conectes a la Internet.
- Permite, que tu software antivirus tenga 'siempre activa' su opción de detección de virus, si cuenta con esta. Es posible que diferentes aplicaciones usen distintos nombres para esta opción pero la mayoría de ellas ofrece una opción como esta. Puede llamarse 'Protección en Tiempo Real,' 'Protección Residente,' o de alguna otra manera similar. Dirígete a la **sección 3.2.1** de la **Guía del Avast** para obtener detalles acerca de la herramienta de 'Escáner por Acceso.'
- Escanea regularmente todos los archivos de tu computadora. No tienes que hacer esto a diario — especialmente si tu software antivirus tiene una opción 'siempre activo', como se describe líneas arriba — pero debes hacerlo de tiempo en tiempo. ¿Cuan a menudo?, dependerá de las circunstancias. ¿Has conectado, recientemente, tu computadora a una red desconocida? ¿Con quien has estado compartiendo tu memoria extraíble USB? ¿Recibes frecuentemente documentos adjuntos extraños con tu correo electrónico? ¿Alguien en tu casa u oficina ha tenido problemas de virus recientemente? Para mayor información de cuál es la mejor manera de escanear archivos, dirígete a la sección de la **Guía del Avast**.

Evitar una infección viral

- Se extremadamente cuidadoso cuando abras archivos adjuntos en tu correo electrónico. Es mejor evitar abrir cualquier archivo adjunto recibido de una fuente desconocida. Si necesitas hacerlo, debes primero guardar el archivo adjunto en una carpeta en tu computadora, luego abrir la aplicación pertinente (tal como Microsoft Word o Adobe Acrobat). Es menos probable que contraigas el virus, si utilizas el menú de Archivo del programa para abrir el archivo adjunto en forma manual, en vez de pulsar dos veces sobre el archivo o permitir que tu programa de correo electrónico lo abra automáticamente.
- Considera los posibles riesgos antes de insertar medios extraíbles, tales como CDs, DVDs y memorias extraíbles USB, en tu computadora. Primero debes verificar que tu programa antivirus tenga las últimas actualizaciones y que su escáner esta ejecutándose. También es una buena idea deshabilitar la opción 'Reproducción Automática' de tu sistema operativo, que puede ser utilizada por los virus para infectar tu computadora. Con el Windows XP, esto puede hacerse dirigiéndote a **Mi PC**, pulsando el botón derecho del ratón sobre tu unidad de CD o DVD, seleccionando **Propiedades** y pulsando sobre la pestaña **Reproducción Automática**. Para cada tipo de contenido, selecciona las opciones, **No realizar ninguna acción** o **Pregúntame siempre que elija una acción** luego pulsa **Aceptar**.
- Puedes también ayudar a evitar algunas infecciones virales cambiándote a un *Software Libre y de Código Abierto (FOSS)*, el cual es a menudo más seguro, y a los cuales los creadores de virus son menos propensos a atacar.

Software Espía (Spyware)

El software espía (spyware) es una clase de *software malicioso (malware)* que puede rastrear el trabajo que haces, tanto en tu computadora como en la Internet, y enviar dicha información a alguien que no debe tener acceso a ella. Estos programas pueden registrar, entre otras cosas, las palabras que digitas en tu teclado, los movimientos de tu ratón, las páginas que visitas y los programas que ejecutas. Como resultado de ello, pueden socavar la seguridad de tu computadora y revelar información confidencial sobre ti, tus actividades y tus contactos. Las computadoras se infectan con software espía (spyware) en prácticamente la misma forma en la que contraen virus, por tanto muchas de las sugerencias realizadas anteriormente son también útiles cuando nos defendemos de esta segunda clase de software malicioso (malware). Debido a que las páginas web maliciosas son la mayor fuente de infecciones de software espía (spyware), debes prestar mayor atención a los sitios web que visitas y asegurarte que las opciones de tu navegador sean seguras.

Assani: Todo eso me suena como algo salido de una película de espías. ¿Mi computadora está en verdad "infectada con software espía (spyware)?"

Muhindo: Lo creas o no, esto es muy común. Si aquellos programas que descargaste de la Internet no te han infectado, existe una buena posibilidad de que por lo menos una de las páginas que has visitado lo haya

hecho. El hecho de que utilices Windows y el Internet Explorer lo hace aun más probable. Si nunca has escaneado tu computadora en busca de software espía (spyware), te apuesto a que te sorprenderás de cuantos están instalados en ella.

Software contra Software espía (spyware)

Puedes utilizar herramientas contra software espía (spyware) para proteger tu computadora de este tipo de amenazas. El *Spybot* es uno de esos programas, y hace un buen trabajo identificando y eliminando ciertos tipos de *software malicioso (malware)* que los programas antivirus simplemente ignoran. Sin embargo, de la misma manera que con un programa antivirus, es extremadamente importante que actualices las definiciones de software malicioso (malware) del Spybot y que ejecutes escaneados regulares.

Evitar infección de software espía (spyware)

- Mantente alerta cuando navegues en sitios web. Cuídate de las ventanas de navegador que aparecen automáticamente, y léelas con cuidado en vez de pulsar simplemente Si o Aceptar. En caso de duda, debes cerrar las 'ventanas emergentes' pulsando la X en la esquina superior derecha, en vez de pulsar sobre Cancelar. Esto puede ayudarte a evitar que las páginas web te engañen instalando *software malicioso (malware)* en tu computadora.
- Mejora la seguridad de tu navegador Web evitando que ejecute automáticamente potenciales programas peligrosos que a veces están contenidos dentro de las páginas web que visitas. Si utilizas Mozilla *Firefox*, puedes instalar el complemento *NoScript*, como se describe en la **sección 4** de la **Guía del Firefox**.
- Nunca aceptes ni ejecutes este tipo de contenido si vienes de un sitio web que no conoces o en el cual no confías.

Assani: He escuchado que los 'Java applets' y los 'controles ActiveX' pueden ser peligrosos. Pero no tengo idea de lo que son.

Salima: Son solo ejemplos de prácticamente lo mismo: pequeños programas que tu navegador Web a veces descarga junto con la página que estás leyendo. Los diseñadores de páginas web los utilizan para crear sitios complejos, pero estos pueden también esparcir virus y software espía (spyware). No tienes porque preocuparte mucho sobre la forma como funcionan, mientras tengas el NoScript instalado y ejecutándose adecuadamente.

Cortafuegos (Firewall)

Un *cortafuegos (firewall)* es el primer programa que encuentran los datos entrantes de Internet. También es el último programa que maneja la información saliente. Como un guardia de seguridad, ubicado en la puerta de un edificio, que decide quien ingresa y quien puede salir, un cortafuegos (firewall) recibe, inspecciona y toma decisiones respecto a la entrada y salida de todos los datos. Naturalmente, es indispensable que te defiendas de conexiones no confiables de Internet y de redes locales, cualquiera de las cuales pueda proporcionar a los *piratas informáticos (hackers)* y a los virus una ruta libre a tu computadora. Sin embargo, el vigilar las conexiones de salida que se originan en tu computadora no es menos importante.

Un buen *cortafuegos (firewall)* te permite elegir permisos de acceso para cada programa en tu computadora. Cuando uno de estos programas intenta contactarse con el exterior, tu cortafuegos (firewall) bloqueará el intento y te enviará una advertencia, a menos que reconozca el programa y verifique que le has dado permiso para que haga ese tipo de conexión. Esto es en gran parte para prevenir que el *software malicioso (malware)* existente esparza virus o invite a *piratas informáticos (hackers)* a ingresar a tu computadora. En este sentido, un cortafuegos (firewall) funciona tanto como una segunda línea de defensa o como un sistema de alerta temprana que puede ayudarte a reconocer cuando la seguridad de tu computadora esta amenazada.

Software Cortafuegos (Firewall)

Las últimas versiones del Microsoft Windows incluyen un *cortafuegos (firewall)* incorporado, que se activa automáticamente. Lamentablemente, el cortafuego de Windows es limitado en muchas formas. Particularmente,

no examina las conexiones de salida y puede ser algo difícil de utilizar. Sin embargo, existe un excelente programa de *software gratuito (freeware)* llamado *Comodo Firewall*, que realiza mejor el trabajo de mantener segura tu computadora.

Evitar conexiones no confiables a red

- Sólo instala programas esenciales, que utilices para trabajo sensible, en tu computadora y asegúrate de obtenerlos de fuentes confiables, Desinstala cualquier software que no utilices.
- Desconecta tu computadora de la Internet cuando no la estés utilizando y desconéctala completamente en la noche.
- No compartas con nadie tu contraseña de Windows.
- Si has habilitado cualquier de los 'servicios de Windows' que ya no estás utilizando, debes deshabilitarlo. Dirígete a la sección de **Lecturas Adicionales** para más detalles sobre esto
- Asegúrate que todas las computadoras de la red de tu oficina tiene instalado un *cortafuegos (firewall)*
- Si todavía no tienes uno, debes considerar instalar un cortafuegos (firewall) adicional para proteger la totalidad de la red local en tu oficina. Muchas de las *pasarelas (gateways)* comerciales de banda ancha incluyen un cortafuegos (firewall) fácil de utilizar, y el ejecutarlo puede mejorar de manera importante la seguridad de tu red. Si no estás seguro como empezar con esto, puede que desees pedir ayuda de quien pueda configurar tu red.

Asani: De modo que ahora, ¿quieren que instale un antivirus, un software contra software espía (spyware) y un software cortafuegos (firewall)? ¿Puede mi computadora arreglárselas con todo eso?

Muhindo: Por supuesto. De hecho, estas tres herramientas son el mínimo indispensable si deseas mantenerte a salvo, en estos días, en la Internet. Estos se han creado para trabajar juntos, de modo que el instalarlos todos no debe causarte ningún problema. Sin embargo, recuerda, no deseas ejecutar dos programas antivirus o dos cortafuegos (firewalls) al mismo tiempo.

Mantener actualizado tu software

Los programas de computadora son a menudo largos y complejos. Es inevitable que algunos de los programas que utilizas regularmente contengan errores no descubiertos, y es probable que algunos de estos errores pudieran socavar la seguridad de tu computadora. Sin embargo, los desarrolladores de software continúan encontrando estos errores, y por ello emiten actualizaciones para arreglarlos. Es por tanto, esencial que actualices frecuentemente todos los programas en tu computadora, incluyendo el sistema operativo. Si Windows no se está actualizando automáticamente, puedes configurarlo para hacerlo pulsando el menú de **Inicio**, seleccionando **Programas** y pulsando **Windows Update**. Esto abrirá el Internet Explorer, y te conducirá a la página de Microsoft Update, donde puedes habilitar la opción de **Actualizaciones Automáticas**. Dirígete a la sección **Lecturas Adicionales** para aprender más acerca de esto.

Mantenerse actualizado con software libre y herramientas de software libre y de código abierto (FOSS)

El *software propietario* a menudo requiere probar que fue comprado legalmente antes de permitirte instalar actualizaciones. Si estás utilizando, por ejemplo, una copia pirata de Microsoft Windows, esta puede no ser capaz de actualizarse automáticamente, lo que te dejaría a ti y a tu información extremadamente vulnerable. Al no tener una licencia válida, te pones a ti y a otros en riesgo. El confiar en software ilegal puede presentar también riesgos no técnicos. Las autoridades en un creciente número de países han empezado a verificar que las organizaciones posean una licencia válida por cada software que utilicen. La policía ha confiscado computadoras y cerrado organizaciones basados en la 'piratería de software.' Esta justificación puede convertirse en un abuso fácilmente en países donde las autoridades tienen razones políticas para interferir en el trabajo de alguna organización determinada. Afortunadamente, no tienes que comprar software costoso para protegerte de tácticas como esta.

Te recomendamos enfáticamente que pruebes *software gratuito (freeware)* o *Software Libre y de Código*

Abierto (FOSS) que sean alternativas a cualquier *software propietario* que utilizas actualmente, especialmente a aquellos programas que no están licenciados. El software gratuito (freeware) y las herramientas de Software Libre y de Código Abierto (FOSS) son a menudo escritos por voluntarios y organizaciones sin fines de lucro que los emiten, e incluso los actualizan, gratuitamente. Las herramientas de Software Libre y Código Abierto (FOSS), en particular, son generalmente considerados más seguros que aquellos software propietarios, debido a que son desarrollados de manera transparente, pues permiten que su *código fuente* sea examinado por un grupo diverso de expertos, cualquiera de los cuales puede identificar problemas y contribuir soluciones.

Muchas aplicaciones de *Software Libre y de Código Abierto (FOSS)* se ven y funcionan de manera casi idéntica al *software propietario* que pretenden reemplazar. Al mismo tiempo, puedes utilizar estos programas junto con el software propietario, incluyendo el sistema operativo Windows, sin ningún problema. Incluso si tus colegas continúan utilizando la versión comercial de un tipo particular de programa, tú puedes intercambiar archivos y compartir información con ellos de manera fácil. En particular, deberías considerar reemplazar el Internet Explorer, Outlook o Outlook Express y Microsoft Office con *Firefox*, *Thunderbird* y OpenOffice, respectivamente.

De hecho, podrías incluso dejar completamente de lado el sistema operativo Microsoft Windows, e intentar utilizar un más seguro *Software Libre y de Código Abierto (FOSS)* alternativo llamado *GNU/Linux*. La mejor manera de saber si estás listo para cambiarte es simplemente intentándolo. Puedes descargar una versión *LiveCD* de *Ubuntu Linux*, quemarla en un CD o DVD, ponerla en tu computadora y reiniciarla. Cuando haya terminado de cargar, tu computadora estará funcionando con GNU/Linux, y podrás decidir que hacer. No te preocupes, nada de esto es permanente. Cuando hayas concluido, simplemente apaga tu computadora y retira el Ubuntu LiveCD. La próxima vez que la enciendas, estarás de vuelta en Windows, y todas tus aplicaciones, configuraciones y datos se encontrarán en la misma forma en la que los dejaste. Además de las ventajas de seguridad general del software de código abierto, Ubuntu tiene una herramienta de actualización libre, de fácil uso que evitará que tu sistema operativo y mucho de tu software queden desactualizados e inseguros.

2. Proteger tu información de amenazas físicas

No importa cuanto esfuerzo hayas puesto en construir una barrera digital alrededor de tu computadora, todavía puedes despertar una mañana y hallar que esta, o una copia de la información en ella, se ha perdido, ha sido robada, o dañada por cualquier serie de accidentes desafortunados o actos maliciosos. Cualquier cosa desde una sobretensión transitoria a una ventana abierta o una taza de café derramada puede conducirte a una situación en la cual todos tus datos se pierdan y no seas capaz de utilizar tu computadora. Una cuidadosa evaluación del riesgo, un consistente esfuerzo para mantener una computadora sin problemas y una *política de seguridad* pueden evitar este tipo de desastre.

Contexto

Shingai y Rudo son una vieja pareja casada con muchos años de experiencia, que ayudan a la población infectada con el VIH en Zimbabwe a mantener su acceso a medicación apropiada. Ellos están postulando para un subsidio para comprar nuevas computadoras y equipo de red para su oficina. Dado que viven en una región que es muy turbulenta, tanto en términos políticos como de infraestructura, ellos y sus potenciales financistas quieren garantizar que su nuevo hardware estará seguro, no sólo de los piratas informáticos (hackers) y los virus, sino también de la confiscación, tormentas eléctricas, picos eléctricos y otros desastres similares. Ellos le consultaron a Otto, un técnico en computadoras local, que les ayude a concebir un plan para reforzar la seguridad física de las computadoras y de los equipos de red que planean adquirir si su solicitud de subvención tiene respuesta.

¿Qué puedes aprender de este capítulo?

- Unos cuantos ejemplos de las muchas *amenazas físicas* a tu computadora y a la información que se halla almacenada en ella.
- Cómo asegurar tu computadora de la mejor forma contra estas amenazas
- Cómo crear un entorno operativo sin problemas para las computadoras y los equipos de red
- Que debes considerar cuando creas un plan de seguridad para las computadoras en tu oficina.

Evaluar tus riesgos

Muchas organizaciones subestiman la importancia de mantener seguras sus oficinas y su equipamiento físico. Como resultado de ello, a menudo carecen de una clara política que describa que medidas deben tomarse para proteger las computadoras y los dispositivos de almacenamiento de respaldos de robos, condiciones climáticas extremas, accidentes, y otras *amenazas físicas*. La importancia de dichas políticas puede parecer obvia, pero el formularlas adecuadamente puede ser más complicado de lo que parece. Muchas organizaciones, por ejemplo, tienen buenas cerraduras en las puertas de sus oficinas — y muchas incluso tienen sus ventanas aseguradas — pero si no prestan atención al número de llaves que han sido creadas, y quienes las tienen, su información sensible se mantendrá vulnerable.

Shingai: Deseamos colocar un breve resumen de nuestra política de seguridad en esta solicitud de subvención, pero también necesitamos asegurarnos que la política es adecuada en si. ¿Qué debemos incluir en ella?

Otto: Me temo que no puedo recomendarle una solución general al reto de la seguridad física. Los detalles de una buena política casi siempre dependen de las circunstancias individuales de la organización en particular. Sin embargo, aquí le brindo algunas consejos generales: cuando intente elaborar un plan, debes observar tu ambiente de trabajo de manera cuidadosa y pensar creativamente sobre donde podrían estar tus puntos débiles y que puedes hacer para fortalecerlos.

Cuando estés evaluando los riesgos y las vulnerabilidades que tú y tu organización afrontan, debes evaluar varios niveles diferentes en los que tus datos pueden estar amenazados.

- Considera los canales de comunicación que usas y cómo lo haces. Ejemplos de ello pueden incluir cartas físicas, faxes, teléfonos fijos, teléfonos móviles, correos electrónicos y mensajes a través de *Skype*.
- Considera cómo almacenas información importante. Los discos duros de las computadoras, los correos electrónicos y los servidores web, las memorias extraíbles USB, los discos duros externos con conexión USB, los CDs y DVDs, los teléfonos móviles, el papel impreso y las notas manuscritas son todas posibilidades.
- Considera donde están ubicados físicamente estos artículos. Pueden estar en la oficina, en la casa, en un bote de basura afuera o, en forma creciente, 'en algún lugar de la Internet.' En este último caso, podría ser todo un reto determinar la ubicación física actual de una pieza particular de información.

Ten en cuenta que la misma pieza de información podría ser vulnerable en distintos niveles. De la misma manera como tú podrías confiar en un software antivirus para proteger los contenidos de una memoria extraíble USB de *software malicioso (malware)*, así también debes confiar en un plan de seguridad física detallado para proteger la misma información del robo, perdida o destrucción. Aunque algunas prácticas de seguridad, tales como tener una buena política de mantener respaldos fuera del lugar de trabajo, son útiles contra amenazas digitales y físicas, otras son claramente más específicas.

Cuando decides llevar tu memoria extraíble USB en el bolsillo o sellada en una bolsa plástica al fondo de tu maleta, estás tomando una decisión de seguridad física, aun cuando la información que tratas de proteger sea digital. Como es normal, la política correcta depende en gran parte de la situación. ¿Estás caminando a través de un pueblo o a través de una frontera? ¿Alguien estará cargando tu bolso o mochila? ¿Está lloviendo? Estas son algunas preguntas que debes tener en cuenta cuando tomes una decisión como esta.

Proteger tu información de intrusos físicos

Los individuos maliciosos que buscan tener acceso a tu información sensible representan una clase importante de *amenaza física*. Sería un error asumir que esta es la única amenaza física a la seguridad de tu información, pero sería aún peor el ignorarla. Existen varios pasos que puedes tomar para ayudar a reducir el riesgo de intrusión física. Las categorías y sugerencias que viene a continuación, muchas de las cuales pueden funcionar tanto para tu domicilio como para tu oficina, representan una base sobre la cual puedes desarrollar otras de acuerdo a tu particular situación de seguridad física.

Alrededor de la Oficina

- Conoce a tus vecinos. Dependiendo del clima de seguridad en tu país y en tu vecindario, una de dos cosas puede ser posibles. Ya sea que, puedas volverlos aliados que te ayudarán a cuidar tu oficina, o personas a las que debes añadir a tu lista de amenazas potenciales y de las cuales debes ocuparte en tu plan de seguridad.
- Revisa como proteges todas tus puertas, ventanas y otros puntos de entrada que conduzcan a tu oficina.
- Considera instalar una cámara de vigilancia o una alarma con sensor de movimiento.
- Trata de crear un área de recepción, donde los visitantes puedan ser contactados antes de que ingresen a la oficina, y una habitación de reuniones que este separada de tu ambiente laboral normal.

En la Oficina

- Protege los cables de red haciéndolos pasar por dentro de la oficina.
- Mantén bajo llave los dispositivos de red como *servidores*, *enrutadores (routers)*, *interruptores*, *concentradores (hubs)*, y módems en habitaciones o gabinetes seguros. Un intruso con acceso físico a dicho equipo puede instalar software malicioso (malware) capaz de robar datos en tránsito o atacar otras computadoras en la red incluso después de que se haya ido.
- Si tienes una red inalámbrica, es esencial que asegures tu *punto de acceso* de modo que los intrusos no puedan unirse a tu red o vigilar tu tráfico. Si estas utilizando una red inalámbrica insegura, cualquiera con una computadora portátil en tu vecindario se convierte en un intruso potencial. Es una definición inusual de riesgo 'físico,' pero ayuda el considerar que un individuo malicioso que pueda vigilar tu red inalámbrica tiene el mismo acceso que uno que pueda ingresar furtivamente en tu oficina y conectar un cable ethernet. Los pasos necesarios para asegurar una red inalámbrica variaran, dependiendo de tu punto de acceso, tu hardware y software, pero son raramente difíciles de seguir.

En tu área de trabajo

- Debes ubicar con cuidado la pantalla de tu computadora, tanto en tu escritorio como cuando estas fuera de la oficina, con el fin de evitar que otros lean los que se muestra en ella. En la oficina, esto significa considerar la ubicación de las ventanas, puertas abiertas y el área de espera de los invitados, si es que cuentas con una.
- La mayoría de las torres (cases) de las computadoras de escritorio tiene una ranura donde puedes colocar un candado que impedirá a alguien sin una llave que pueda tener acceso a su interior. Si tienes torres (cases) como esta en la oficina, debes colocarles candados de modo que los intrusos no puedan alterar el hardware interno. Esta característica debe ser considerada al momento de comprar nuevas computadoras.
- Utiliza un cable de seguridad de cierre, cuando sea posible, para evitar que intrusos puedan robar las computadoras en sí. Esto es especialmente importante para computadoras portátiles y pequeñas computadoras de escritorio que pueden ser escondidas en una bolsa o bajo un abrigo.

Software y configuraciones relacionadas a la seguridad física

- Asegúrate que, cuando reinicies tu computadora, esta te solicite una contraseña antes de permitirte ejecutar un software y acceder a archivos. Si no lo hace, puedes habilitar esta opción en Windows pulsando el Menú de Inicio, Configuración, seleccionar el Panel de Control, y pulsar dos veces en Cuentas de Usuario. En la pantalla de Cuentas de Usuario, selecciona tu cuenta y pulsa en Crear una Contraseña. Elige una contraseña segura, como se discute en el capítulo **3. Crear y mantener contraseñas seguras**, ingresa tu contraseña, confírmala, pulsa Crear Contraseña y pulsa Si, Hacerla Privada (Make Private).
- Existen pocas opciones en el *BIOS* de tu computadora que sean pertinentes para la seguridad física. Primero, debes configurar tu computadora de modo que no *arranque* desde una unidad de disquete, CD-ROM o DVD. Segundo, debes fijar una contraseña en el mismo BIOS, de modo que un intruso no pueda simplemente deshacer la configuración previa. Nuevamente, asegúrate de elegir una contraseña segura.
- Si confías en una base de datos de contraseñas seguras, como se aborda en el **capítulo 3**, para almacenar tus contraseñas de Windows o del BIOS para una computadora en particular, asegúrate de no guardar tu

copia única de la base de datos en dicha computadora.
- Adquiere el hábito de cerrar tu cuenta cada vez que te alejes de tu computadora. En Windows, puedes hacer esto rápidamente manteniendo presionada la tecla con el logo de Windows y presionando la tecla L. Ello solo funcionará si has creado una contraseña para tu cuenta, como se describió anteriormente.
- *Cifra* la información sensible en tus computadoras y dispositivos de almacenamiento en tu oficina. Dirígete al capítulo **4. Proteger los archivos sensibles en tu computadora** para obtener detalles e indicaciones adicionales en las Guías Prácticas pertinentes.

Rudo: Estoy un poco nervioso en cuanto a equivocarme en el BIOS. ¿Podría malograr mi computadora si cometo algún error?

Otto: Si puedes, al menos por un instante. De hecho, las opciones que desearías cambiar son muy simples, pero la pantalla del BIOS puede ser un poco intimidante, y es posible dejar tu computadora temporalmente incapaz de arrancar si cometes algún error. En general, si no te sientes cómodo trabajando en el BIOS, debes pedir a alguien con mayor experiencia con computadoras que te ayude.

Dispositivos Portátiles

- Mantén tu computadora portátil, tu teléfono móvil y otros dispositivos portátiles que contengan información sensible todo el tiempo contigo, especialmente si estas viajando o te estas alojando en un hotel. El viajar con un *cable de seguridad* para computadora portátil es una buena idea, aunque a veces es difícil encontrar un objeto apropiado al cual puedas fijarlo. Recuerda que las horas de toma de alimentos son a menudo aprovechadas por los ladrones, muchos de los cuales han aprendido revisar cuartos de hotel en busca de computadoras portátiles durante las horas del día cuando estas están probablemente sin vigilancia.
- Si tienes una computadora portátil o un dispositivo de cómputo portátil, tal como un Asistente Personal Digital (PDA), trata de evitar ponerlos a vista de todos. No hay necesidad de mostrar a los ladrones que estas llevando valioso hardware o de mostrarles a los individuos que pudieran desear acceder a tus datos, que tu mochila contiene un disco duro lleno de información. Evita usar tus dispositivos portátiles en áreas públicas, y considera llevar tu computadora portátil en algo que no se vea como una bolsa para computadoras portátiles.

Mantener un ambiente sano para el hardware de tu computadora

Como muchos dispositivos electrónicos, las computadoras son muy sensibles. No se adaptan bien a la inestabilidad eléctrica, temperaturas extremas, polvo, alto grado de humedad o esfuerzo mecánico. Existen muchas cosas que puedes hacer para proteger a tu computadora y el equipo de tu red de dichas amenazas:

- Los problemas eléctricos tales como sobrecargas de energía, apagones y bajas de tensión pueden causar daño físico a una computadora. Las irregularidades como estas pueden 'hacer fallar' tu disco duro, dañar la información que contiene, o dañar físicamente los componentes eléctricos en tu computadora.
  - Si puedes costearlas, debes instalar dispositivos de *Corriente Eléctrica Ininterrumpida* (UPS por sus siglas en inglés) en las computadoras más importantes de tu oficina. Un UPS proporciona energía temporal en caso de apagón.
  - Incluso donde las *UPSs* se consideran inapropiadas o muy costosas, puedes proporcionar filtros de energía o protectores contra sobretensiones, cualquiera de los cuales ayudará a proteger tus equipos de sobrecargas de energía.
  - Prueba tu red eléctrica antes de conectar equipos importantes a ella. Trata de usar enchufes que tengan tres ranuras, una de ellas 'a tierra.' Y, si es posible, tómate un día o dos para ver como se comporta el sistema eléctrico en una nueva oficina cuando está dando energía a dispositivos baratos, tales como lámparas y ventiladores, antes de poner tus computadoras en riesgo.
- Para protegerse contra los accidentes en general, evita colocar hardware importante en pasillos, áreas de recepción, u otras ubicaciones de fácil acceso. Los *UPSs*, filtros de energía, protectores contra

sobretensiones, múltiples y cables de extensión — particularmente aquellos conectados a los servidores y al equipo de red — deben estar ubicados donde no puedan ser apagados por un traspié accidental.
- Si tienes acceso a cables de computadora, múltiples y cables de extensión de alta calidad, debes comprar suficientes para servir a toda la oficina y contar con algunos extras. Los múltiples que se desprenden de enchufes en las paredes, no sostienen bien los enchufes y producen chispas constantemente son más que molestos. Estos pueden ser muy perjudiciales para la seguridad física de cualquier computadora que esté conectada a este. Ello puede conducir a que usuarios frustrados aseguren sus cables sueltos a múltiples utilizando cinta adhesiva, lo cual crea un obvio peligro de incendio.
- Si mantienes alguna de tus computadoras dentro de un gabinete, asegúrate que tengan ventilación adecuada, o sino se pueden sobrecalentar.
- El equipo de computación no debe ser ubicado cerca de radiadores, rejillas de la calefacción, acondicionadores de aire u otros conductos

3. Crear y mantener contraseñas seguras

Muchos de los servicios seguros que nos permiten sentirnos cómodos utilizando la tecnología digital para conducir negocios importantes, desde ingresar a nuestras computadoras y enviar correos electrónicos hasta *cifrar* y esconder datos sensibles, requieren que recordemos una contraseña. Estas palabras secretas, frases o secuencias en auténtico galimatías a menudo proporcionan la primera, y a veces la única, barrera entre tu información y cualquiera que pudiera leerla, copiarla, modificarla o destruirla sin permiso. Existen muchas maneras por las cuales alguien puede descubrir tus contraseñas, pero puedes defenderte de la mayoría de ellos aplicando unas cuantas tácticas y por medio de una herramienta de *base de datos de contraseñas seguras*, tales como el *KeePass*.

Contexto

Mansour y Magda son dos hermanos, en un país de habla árabe, quiénes mantienen una bitácora (blog) en la cual anónimamente hacen difusión sobre abusos de los derechos humanos y hacen campañas para un cambio político. Magda recientemente trató de conectarse a su cuenta de correo con interfase web y se encontró con que su contraseña había sido modificada. Después de reestablecer la contraseña, ella fue capaz de conectarse, pero cuando abrió su buzón encontró que muchos mensajes nuevos fueron marcados como leídos. Ella sospecha que alguien afiliado a una organización de adversarios políticos pudiera haber descubierto o adivinado su contraseña, la cual utiliza para prácticamente todas sus cuentas web. Ella se reúne con Mansour, que tiene menor experiencia con computadoras, para explicarle la situación y expresarle su preocupación.

¿Qué puedes aprender de este capítulo?

- Los elementos de una contraseña segura
- Unos cuantos trucos para recordar contraseñas largas y complicadas
- Cómo utilizar la *base de datos de contraseñas seguras* del *KeePass* para almacenar contraseñas en vez de recordarlas

Seleccionar y mantener contraseñas seguras

En general, cuando deseas proteger algo, lo cierras con una llave. Las cerraduras de las casas, automóviles y bicicletas tienen llaves físicas; los archivos protegidos tienen llaves de *cifrado*; las tarjetas bancarias tiene números PIN; y las cuentas de correo electrónico tienen contraseñas. Todas estas llaves, en forma literal y metafórica, tienen una cosa en común: abren sus respectivas cerraduras con la misma eficacia en manos de otra persona. Puedes instalar cortafuegos avanzados, cuentas de correo electrónico seguras, y discos cifrados, pero si tu contraseña es muy débil, o si permites que caiga en las manos equivocadas, ello no te hará mucho bien.

Elementos de una contraseña sólida

Una contraseña debe ser difícil de adivinar para un programa de computadora.

- **Debe ser larga**: Cuanto más larga es la contraseña es menos probable que sea adivinada por un programa de computadora en un tiempo razonable. Debes tratar de crear contraseñas que incluyan diez o más caracteres. Algunas personas utilizan contraseñas que contienen más de una palabra, con o sin espacios, las cuales son a menudo llamadas frases contraseña. Esta es una buena idea, en la medida que el programa o servicio que utilices te permita elegir contraseñas lo suficientemente largas.
- **Debe ser compleja**: Además de ser extensa, la complejidad de una contraseña también ayuda a evitar que el software automático de 'descifrado de contraseñas' adivine la correcta combinación de caracteres. Donde sea posible, siempre debes incluir en tu contraseña letras en mayúsculas, en minúsculas, números, y símbolos tales como signos de puntuación.

Una contraseña debe ser difícil de descifrar para otros.

- **Debe ser práctica:** Si has escrito tu contraseña debido a que no puedes recordarla, podrías terminar afrontando una completamente nueva categoría de amenazas que te podría dejar vulnerable ante cualquiera con una clara vista de tu escritorio o acceso temporal a tu domicilio, tu billetera, o incluso el bote de basura fuera de tu oficina. Si eres incapaz de pensar en una contraseña que sea larga y compleja pero a la vez factible de ser recordada, la sección **Recordar y registrar contraseñas seguras**, que viene a continuación, podría ser de ayuda. Sino, debes todavía escoger algo seguro, pero necesitas registrarla utilizando una *base de datos de contraseñas seguras* tal como *KeePass*. Otros tipos de archivos protegidos por contraseña, incluyendo documentos de Microsoft Word, no debe ser confiados para este propósito, debido a que muchos de ellos pueden ser descifrados en segundos utilizando herramientas que son de libre acceso en Internet.
- **No debe ser personal:** Tu contraseña no debe estar relacionada a ti de manera personal. No elijas una palabra o frase que se origina de información como tu nombre, número de seguridad social, número de teléfono, nombre de tu hijo(a), nombre de tu mascota, fecha de nacimiento, o cualquier otra cosa que una persona podría descubrir haciendo una pequeña investigación sobre ti.
- **Debe mantenerse secreta:** No compartas tu contraseña con nadie a menos que sea absolutamente necesario. Y, si debes compartir una contraseña con un amigo, miembro de la familia o colega, debes cambiarla a una contraseña temporal primero, compartir esta, luego cambiarla nuevamente cuando la persona haya terminado de utilizarla. A menudo, existen alternativas para compartir una contraseña, tal como crear una cuenta separada para cada miembro que necesite acceso. El mantener tu contraseña secreta también implica poner atención a quién podría estar fisgoneándote cuando la ingresas o buscas en una *base de datos de contraseñas seguras*.

Una contraseña debe ser escogida de modo que se minimice el daño si alguien la descubre.

- **Hazla única:** Evita usar la misma contraseña para más de una cuenta. De otro modo, cualquiera que descubra dicha contraseña tendrá acceso a incluso mayor información sensible. Esto es particularmente cierto debido a que ciertos servicios hacen relativamente simple descifrar tu contraseña. Si utilizas, por ejemplo, la misma contraseña para tu cuenta de usuario de Windows y para tu cuenta de Gmail, alguien con acceso físico a tu computadora puede descifrar la primera y utilizarla para acceder a la segunda. Por razones similares, es una mala idea el rotar contraseñas intercambiándolas entre diferentes cuentas.
- **Mantenla siempre nueva:** Cambia tu contraseña de manera regular, de manera preferente una vez cada tres meses. Algunas personas son muy apegadas a una contraseña en particular y nunca la cambian. Esta es una mala idea. Cuanto más tiempo mantienes una contraseña, existe mayor oportunidad de que otros la descubran. Además, si alguien es capaz de utilizar tu contraseña (robada) para acceder a tu información y servicios sin que lo sepas, está continuará haciéndolo hasta que la cambias.

Mansour: ¿Qué ocurre en el caso que confíe en una persona? Está bien si te confío mi contraseña, ¿cierto?

Magda: Bueno, en primer lugar, solo porque confíes en alguien para darle tu contraseña no significa que confíes en esa persona para cuidar de ella, ¿cierto? Aunque yo no haría nada malo con tu contraseña, podría escribirla y perderla o cualquier otra cosa. Después de todo, ¡esa podría ser la forma como me metí en este problema! Además, no todo es cuestión de confianza. Si tú eres la única persona que conoce la contraseña,

entonces no tienes que perder el tiempo preocupándote de a quién culpar si alguien entró sin autorización a tu cuenta. En este momento, por ejemplo, en vez de estar interrogándolos, estoy casi seguro que alguien en realidad adivinó o 'descifró' mi contraseña.

Recordar y registrar contraseñas seguras

Examinando la lista de sugerencias dada anteriormente, te preguntarás cómo puede alguien sin memoria fotográfica estar al tanto de contraseñas que son largas, complejas y sin sentido, si es que no las escribe. La importancia de utilizar diferentes contraseñas para cada cuenta lo hace aún más difícil. Sin embargo, existen algunos trucos que pueden ayudarte a crear contraseñas que son fáciles de recordar pero extremadamente difíciles de adivinar, incluso para una persona inteligente utilizando un programa avanzado de 'descifrado de contraseñas'. También tienes la opción de registrar tus contraseñas utilizando una de las *bases de datos de contraseñas seguras*, tal como el *KeePass*, que fue específicamente creado para este propósito.

Recordar contraseñas seguras

Es importante utilizar diferentes tipos de caracteres cuando escojas una contraseña. Esto se puede realizar de distintas maneras:

- Utilizando mayúsculas y minúsculas, tal como: 'Mi nomBRE NO es SR. MarSter?'
- Intercalando números y letras, tal como: 'a11 w0Rk 4nD N0 p14Y'
- Incorporando ciertos símbolos, tal como: 'c@t(heR1nthery3'
- Utilizando diferentes idiomas, tal como: 'Let Them Eat 1e gateaU du ch()colaT'

Cualquiera de estos métodos puede ayudarte a incrementar la complejidad de una contraseña. Obviamente, esto no hará fácil de recordar una contraseña normal, pero te permitirá elegir una contraseña más segura sin tener que entregarte completamente a la idea de memorizarla por completo. Algunas de las sustituciones más comunes (tales como utilizar cero en vez de una 'o' o el símbolo '@' en lugar de 'a') fueron hace mucho incorporados en las herramientas de descifrado de contraseñas, pero aún así son todavía una buena idea. Estas incrementan la cantidad de tiempo que dichas herramientas requerirían para descubrir la contraseña y, en las situaciones más comunes en las que herramientas de esta clase no pueden ser utilizadas, estás evitan las afortunadas adivinanzas.

Las contraseñas pueden también aprovechar las ventajas de *códigos nemotécnicos* más tradicionales, tales como el uso de acrónimos. Esto permite que largas frases se conviertan en palabras complejas y prácticamente aleatorias:

- '¿Ser o no ser? Esa es la pregunta' se convierte en 'So-S?ElaP'
- 'Sostenemos como evidentes por sí mismas dichas verdades: que todos los hombres son creados iguales' se convierte en 'Scepsmdv:q’thsc=s'
- '¿Estás feliz hoy?' se convierte en 'tas:-)h0y?'

Estos son solo unos cuantos ejemplos para ayudarte a desarrollar tu propio método de cifrar palabras y frases para hacerlas simultáneamente complejas y memorables.

Registrar contraseñas de forma segura

Mientras que un poco de creatividad te permitirá recordar todas tus contraseñas, la necesidad de cambiarlas periódicamente significa que muy pronto se te puede acabar la creatividad. Como alternativa, puedes generar contraseñas aleatorias y seguras para la mayoría de tus cuentas y simplemente dedicarte a recordarlas todas. En lugar de ello, puedes registrarlas en una *base de datos de contraseñas seguras* portátil y cifrada tal como el *KeePass*.

Por su puesto, si utilizas este método, se hace especialmente importante que creas y recuerdes una contraseña muy segura para el *KeePass*, o cualquiera que sea la herramienta que elijas. Cuando sea que necesites ingresar una contraseña para una cuenta específica, puedes encontrarla utilizando sólo tu contraseña maestra, la cual hace más fácil seguir todas las sugerencias que se hicieron anteriormente. El KeePass es también portátil, lo que significa que también puedes colocar tu base de datos en una memoria extraíble USB en caso necesites buscar contraseñas cuando estás alejado de tu computadora principal.

Aunque es probablemente la mejor opción para cualquiera que tenga que mantener un gran número de cuentas, existen algunos inconvenientes para este método. Primero, si pierdes o accidentalmente borras tu única copia de tu base de datos de contraseñas, no tendrás más acceso a ninguna de tus cuentas de las cuales esta tenía la contraseña. Esto hace extremadamente importante que hagas una copia de seguridad o respaldo de tu base de datos del *KeePass*. Revisa el capítulo **5. Recuperar información perdida** para mayor información sobre estrategias para la copia de seguridad o respaldo. Felizmente, el hecho que tu base de datos esté cifrada significa que no tienes que entrar en pánico si pierdes tu memoria extraíble USB o una unidad de respaldo que contenga una copia de este.

El segundo gran inconveniente podría ser más importante. Si olvidas tu contraseña maestra del *KeePass*, no existe un modo de recuperarla o recuperar los contenidos de tu base de datos. Por tanto, ¡asegúrate de escoger una contraseña maestra que sea tanto segura como memorable!

Mansour: Espera un minuto. Si el KeePass utiliza una sola contraseña maestra para proteger todas tus demás contraseñas, ¿cómo es más seguro que simplemente utilizar la misma contraseña para todas tus cuentas? Es decir, si una mala persona toma conocimiento de mi contraseña maestra, entonces tendrá acceso a todo, ¿cierto?

Magda: Es un buen razonamiento, y tienes razón al decir que proteger tu contraseña maestra es en verdad importante, pero existen un par de diferencias claves. En primer lugar, esta 'mala persona' no solo necesitaría tu contraseña, él también necesitaría tu archivo de base de datos del KeePass. Si tú simplemente compartes la misma contraseña con todas tus cuentas, el simplemente necesitaría sólo tu contraseña. Más importante aún, sabemos que el KeePass es extremadamente seguro, a diferencia de otros programas y sitos web del medio. Tú no deseas, por ejemplo, a alguien incursionando en un sitio web inseguro y luego que utilice lo que descubrió para acceder a una cuenta más segura. Y, finalmente, el KeePass hace que sea fácil cambiar tu contraseña maestra si crees que esta ha quedado 'comprometida.' ¡Sería tan afortunado! Me pase todo el día cambiando contraseñas de sitios web.

4. Proteger los archivos sensibles en tu computadora

El acceso no autorizado a la información en tu computadora o dispositivo de almacenamiento portátil puede llevarse a cabo de manera remota, si el 'intruso' es capaz de leer o modificar tus datos a través de la Internet, o físicamente, si logra conectarse con tu hardware. Puedes protegerte de cualquiera de estos tipos de amenaza mejorando la seguridad física y de la red de tu datos, como se trató en el capítulo **1. Proteger tu computadora de software malicioso (malware) y de piratas informáticos (hackers)** y en el capítulo **2. Proteger tu información de amenazas físicas**.

Sin embargo, es siempre mejor tener varios niveles de defensa, razón por la cual debes proteger también los archivos mismos. De esta manera, es probable que tu información sensible se mantenga a salvo incluso si tus otras iniciativas en seguridad resultan ser inadecuadas.

Existen dos enfoques generales frente al reto de dar seguridad a tus datos en esta forma. Puedes *cifrar* tus archivos, haciéndolos ilegibles a cualquiera que no sea tú, o puedes esconderlos confiando en que un intruso será incapaz de encontrar tu información sensible. Existen herramientas que te ayudan con cualquiera de los enfoques, incluyendo una aplicación que es un *Software Libre y de Código Abierto (FOSS)* llamado *TrueCrypt*, que puede tanto cifrar como esconder tus archivos.

Contexto

Claudia y Pablo trabajan con una ONG de derechos humanos en un país de Sudamérica. Ellos han pasado muchos meses recolectando testimonios de testigos de violaciones de los derechos humanos que fueron cometidos por el ejército en su región. Si los detalles de quién proporcionó estos testimonios se hacen conocidos se pondría en peligro tanto a la valerosa gente que testificó, como a los miembros de la organización en dicha región.

Esta información está actualmente almacenada en una hoja de cálculo en la computadora de la ONG que funciona con Windows XP, la cual está conectada a Internet.Siendo concientes de la seguridad, Claudia se ha asegurado de almacenar en un CD una copia de respaldo de los datos, este se mantiene fuera de la oficina.

¿Qué puedes aprender de este capítulo?

- Cómo *cifrar* información en tu computadora
- Cuales son los riesgos que podrías afrontar manteniendo tus datos cifrados
- Cómo proteger datos en memorias extraíbles USB, en caso estas se pierdan o sean robadas
- Que pasos debes dar para esconder información de intrusos físicos y remotos

Cifrar tu información

Pablo: ¡Pero mi computadora ya está protegida por la contraseña de acceso de Windows! ¿No es eso lo suficientemente bueno?

Claudia: En realidad, las contraseñas de acceso de Windows son normalmente muy fáciles de descifrar. Además, cualquiera que ponga sus manos en tu computadora por el tiempo suficiente para reiniciar tu computadora con un LiveCD en la unidad lectora puede copiar tus datos sin siquiera tener que preocuparse sobre la contraseña. Si esta persona logra llevarse la computadora por un momento te encontrarás en peores problemas. Por ello no es sólo de la contraseña de Windows de lo que necesitas preocuparte. Tampoco debes confiar en las contraseñas de Microsoft Word o de Adobe Acrobat.

El *cifrar* tu información se parece un poco a mantenerla encerrada en una caja fuerte. Sólo aquellos que tengan la llave o conozcan la combinación de la cerradura pueden acceder a ella. La analogía es particularmente apropiada para el *TrueCrypt* y herramientas similares, las cuales crean contenedores seguros llamados 'volúmenes cifrados' en vez de simplemente proteger un archivo a la vez. Puedes poner un gran número de archivos dentro de un volumen cifrado, pero estas herramientas no protegerán nada que esté almacenado en otro lugar en tu computadora o en tu memoria extraíble USB.

Mientras que otro software puede proporcionarte un *cifrado* que sea igualmente sólido, *TrueCrypt* fue diseñado específicamente para hacer de este tipo de almacenamiento seguro lo más simple posible. Adicionalmente, proporciona respaldo para llevar volúmenes cifrados en dispositivos portátiles de almacenamiento, el hecho de que sea una herramienta de *Software Libre y de Código Abierto (FOSS)*, y su opción de 'denegación' descrita en la sección - que viene a continuación - **Ocultar tu información sensible** le da al TrueCrypt una ventaja distinta sobre muchas herramientas de cifrado incorporadas, de *software propietario*, tales como el 'bitlocker' de Windows XP.

Pablo: Está bien, ahora si que me tienes preocupado. ¿Qué sucede con los otros usuarios de la misma computadora? ¿Esto significa que pueden leer documentos en la carpeta de 'Mis Documentos'?

Claudia: ¡Me gusta la manera en la que piensas! Si tu contraseña de Windows no te protege de los intrusos, ¿Cómo te podría proteger de otras personas con cuentas en la misma computadora?.

De hecho, tu carpeta de Mis Documentos está normalmente visible para cualquiera, de modo que otros usuarios no tendrían siquiera que hacer algo inteligente para leer tus archivos no cifrados. Sin embargo, tienes razón, incluso si la carpeta se hace 'privada,' todavía no estás a salvo a menos que utilices algún tipo de cifrado.

Consejos para utilizar el cifrado de archivos de manera segura

Almacenar datos confidenciales puede ser un riesgo para ti y para con quienes trabajas. El *cifrado* reduce el riesgo pero no lo elimina. El primer paso para proteger información sensible es el reducir cuanto de ella mantienes a tu alrededor. A menos que tengas una buena razón para almacenar un archivo en particular, o una categoría particular de información dentro de un archivo, tú simplemente debes borrarla. (Dirígete al capítulo **6. Destruir información sensible** para obtener mayor información de como hacerlo de manera segura.) El segundo paso es utilizar una buena herramienta de cifrado de archivos, tal como el *TrueCrypt*.

Claudia: Bien, tal vez no necesitamos en realidad almacenar información que podría identificar a las personas que nos dieron sus testimonios. ¿Qué opinas?

Pablo: De acuerdo. Probablemente deberíamos escribir lo menos posible sobre ello. Además, deberíamos pensar en un código simple que podamos utilizar para proteger los nombres y las ubicaciones que tenemos que registrar de todas maneras.

Regresando a la analogía de la caja fuerte cerrada, hay algunas cosas que debes tener en cuenta cuando utilices el *TrueCrypt* u otras herramientas similares. No importa cuan robusta sea tu seguridad, no te hará mucho bien el dejar la puerta abierta. Cuando tu volumen TrueCrypt está 'montado' (el momento en que puedes acceder a su contenido), tus datos pueden ser vulnerables, de modo que debe mantenerse cerrado excepto cuando estás, ciertamente, leyendo o modificando los archivos dentro de este.

Existen algunas situaciones en las que es especialmente importante que recuerdes no dejar montado tu volumen *cifrado*:

- Desconéctalo cuando debas alejarte de tu computadora por cualquier lapso de tiempo. Incluso si normalmente dejas tu computadora funcionando toda la noche, debes asegurarte de no dejar tus archivos sensibles accesibles a intrusos físicos o remotos mientras estás ausente.
- Desconéctalo antes de poner tu computadora a dormir. Esto se aplica a las opciones de 'suspendido' e 'hibernación', las cuales son comúnmente usadas con las computadoras portátiles pero que pueden estar presentes también en las computadoras de escritorio.
- Desconéctalo antes de permitir a alguien manejar tu computadora. Cuando pases tu computadora portátil a través de un control de seguridad o frontera, es importante que desconectes todos los volúmenes *cifrados* y que apagues completamente tu computadora.
- Desconéctalo antes de insertar una memoria extraíble USB no confiable u otro dispositivo de almacenamiento externo, incluyendo aquellos que pertenezcan a amigos y colegas.
- Si mantienes un volumen *cifrado* en una memoria extraíble USB, recuerda que el solo hecho de remover el dispositivo puede no desconectar inmediatamente el volumen. Incluso si necesitas mantener seguros tus archivos cuando estás apurado tienes que desmontar el volumen de forma apropiada, luego desconectar la unidad externa o la memoria extraíble, y luego retirar el dispositivo. Podrías desear practicar hasta que halles la forma más rápida de hacer todas estas cosas.

Si decides mantener tu volumen *TrueCrypt* en una memoria extraíble USB, también puedes mantener una copia del programa TrueCrypt en ella. Esto te permitirá tener acceso a tus datos en las computadoras de otras personas. Sin embargo, las reglas normales todavía se aplican: si no confías en que la máquina esté libre de *software malicioso (malware)*, probablemente no deberías ingresar tus contraseñas o acceder a datos sensibles.

Ocultar tu información sensible

Un problema con el hecho de mantener una caja fuerte en tu casa u oficina, ni que decir de portarla, es que tiende a ser muy obvio. Muchas personas tienen preocupaciones razonables sobre autoincriminarse por medio del uso del *cifrado*. Sólo porque las razones legítimas para cifrar datos exceden en número aquellas ilegítimas no hace esta amenaza menos real. Existen dos razones fundamentales por las que tú podrías evitar utilizar una herramienta como el *TrueCrypt*: el riesgo de autoincriminación y el riesgo de identificar claramente la ubicación de tu información más sensible.

Considerar el riesgo de autoincriminación

El *cifrado* es ilegal en algunos países, lo que significa que descargar, instalar o utilizar software de este tipo podría ser un crimen en si. Y, si la policía, el ejército o los servicios de inteligencia se hallan entre los grupos de quienes estás buscando proteger tu información, entonces el violar estas leyes puede proporcionarles un pretexto ideal bajo el cual tus actividades pueden ser investigadas o tu organización perseguida. En realidad, amenazas como esta pueden no tener nada que ver con la legalidad de las herramientas en cuestión. En cualquier momento, el mero hecho de estar asociado con software de cifrado sería suficiente para exponerte a acusaciones de actividad criminal o espionaje—sin importar lo que realmente está dentro de los volúmenes cifrados-- por tanto debes pensar cuidadosamente respecto a si dichas herramientas son apropiadas o no para tu situación.

Si ese es el caso, tú tienes unas cuantas opciones:

- Puedes evitar completamente el utilizar software de seguridad de datos, lo que requerirá que almacenes información no confidencial o inventes un sistema de palabras códigos para proteger elementos clave de tus archivos sensibles.
- Puedes confiar en una técnica llamada *esteganografía* para esconder tu información sensible, en vez de cifrarla. Existen herramientas que pueden ayudarte con ello, pero el utilizarlas adecuadamente requiere una preparación muy cuidadosa, y todavía corres el riesgo de incriminarte a los ojos de cualquiera que descubra que herramienta estás utilizando.
- Puedes intentar almacenar toda tu información sensible en una cuenta de correo electrónico con interfaz web segura, pero ello requiere de una conexión de red confiable y un relativamente sofisticado nivel de conocimiento de computadoras y de servicios de Internet. Esta técnica también asume que el *cifrado* de red es menos incriminatorio que el cifrado de archivos y que no puedes evitar accidentalmente copiar datos sensibles en tu disco duro y dejarla ahí.
- Puedes mantener la información sensible lejos de tu computadora almacenándola en una memoria extraíble USB o en una disco duro portátil. Sin embargo, tales dispositivos son normalmente incluso más vulnerables que las computadoras a la perdida y a su confiscación, de modo que estar portando información sensible y no cifrada en uno de estos tipos de dispositivos es normalmente una mala idea.

Si es necesario, puedes emplear varias de estas tácticas. Sin embargo, incluso en circunstancias en las que estás preocupado sobre la autoincriminación, lo más seguro será utilizar el *TrueCrypt*, mientras tratas de camuflar tu volumen *cifrado* de la mejor manera posible.

Si deseas que tu volumen cifrado sea menos llamativo, puedes renombrarlo para que se parezca a un tipo diferente de archivo. Utiliza la extensión '.iso', para camuflarlo como una imagen de CD, es una opción que funciona bien para grandes volúmenes de alrededor de 700 MB. Otras extensiones serían más realistas para pequeños volúmenes. Esto se asemeja a esconder tu caja fuerte detrás de una pintura en la pared de tu oficina. Este no será útil bajo inspección detallada, pero ofrecerá alguna protección. También puedes renombrar el mismo programa *TrueCrypt*, asumiendo que lo has guardado como harías con un archivo normal en tu disco duro o memoria extraíble USB, en vez de instalarlo como programa. La **guía del TrueCrypt** te explica cómo hacerlo.

Considerar el riesgo de identificar tu información sensible

A menudo, debes preocuparte menos de las consecuencias de ser 'capturado' con software de *cifrado* en tu computadora o en tu memoria extraíble USB y hacerlo más porque tu volumen cifrado indique específicamente donde almacenas la información que deseas proteger más. Aunque pueda ser cierto que nadie más pueda leerla, un intruso sabrá que está ahí, y que has dado pasos para protegerla. Ello te expone a varios métodos no técnicos a través de los cuales dicho intruso podría intentar tener acceso, ello incluye la intimidación, el chantaje, la interrogación y la tortura. Es en este contexto que la opción o característica de denegación del *TrueCrypt*, que se trata detalladamente más adelante, entra en juego.

La opción de denegación del *TrueCrypt* es una de las maneras en las cuales este va más allá de lo ofrecido por las herramientas de *cifrado* de archivos. Esta opción puede interpretarse como una forma peculiar de *esteganografía* que disfraza tu información más sensible como otra, menos sensible, información oculta. Es análogo a instalar un astuto 'falso fondo' dentro de una no tan sútil caja fuerte. Si un intruso se roba tus llaves, o te intimida para que le des la combinación de la caja fuerte, este encontrará algún material de 'señuelo'

convincente, pero no la información que realmente te importa proteger.

Sólo tú sabes que tu caja fuerte contiene un compartimiento oculto en su parte trasera. Esto te permite 'negar' que estás manteniendo algún secreto más allá de lo que ya le has dado al intruso, y podría ayudar a protegerte en situaciones en las cuales por alguna razón debes reveler una contraseña. Tales razones podrían incluir amenazas legales o físicas a tu propia seguridad, o aquella de tus colegas, asociados, amigos y familiares. El propósito de la denegación es el de darte una oportunidad de escapar de una situación potencialmente peligrosa incluso si decides continuar protegiendo tus datos. Sin embargo, como se trata en la sección de **Considerar el riesgo de la autoincriminación**, esta opción es mucho menos útil si el mero hecho de ser capturado con una caja fuerte en tu oficina es suficiente para provocar consecuencias inaceptables.

La opción de denegación del TrueCrypt funciona por medio del almacenamiento de un 'volumen oculto' dentro de un volumen común *cifrado*. Este volumen oculto se abre proporcionando una contraseña alterna diferente a la que normalmente utilizarías. Incluso si un intruso técnicamente sofisticado logra acceder a tu volumen común, él será incapaz de probar que existe uno oculto. Por supuesto, el puede muy bien saber que el *TrueCrypt* es capaz de ocultar información de esta forma, de modo que no hay garantía de que la amenaza desaparezca tan pronto como reveles tu contraseña señuelo. Muchas personas utilizan el TrueCrypt sin habilitar su opción de denegación, sin embargo, se considera en general que es imposible determinar, a través de un análisis, si un volumen cifrado contiene esta clase de 'falso fondo'. Eso nos dice, que es tu trabajo asegurarte de no revelar tu volumen oculto por medio de medios menos técnicos, tales como dejarlo abierto o permitir que otras aplicaciones creen accesos directos a los archivos que contiene. La sección de **Lecturas Adicionales**, que viene a continuación, te puede dirigir a obtener mayor información al respecto.

Claudia: Bien, entonces vamos a arrojar algo de basura dentro del volumen común, y luego, podemos desplazar todos nuestros testimonios dentro del volumen oculto. ¿Tienes algunos viejos PDFs o algo que podamos utilizar?

Pablo: Justamente estuve pensando en ello, es decir, la idea es revelar la contraseña señuelo si no tenemos otra opción, ¿cierto? Pero para que ello sea convincente, necesitamos asegurarnos que dichos archivos se vean importantes, ¿no crees? De otro modo, ¿Por qué nos molestaríamos en cifrarlos? Tal vez deberíamos utilizar algunos documentos financieros no relacionados o una lista de contraseñas de sitios web o algo parecido.

5. Recuperar información perdida

Cada nuevo método de almacenamiento o transferencia de información digital tiende a introducir muchas más formas nuevas en las que la información en cuestión puede perderse, ser capturada o destruida. Años de trabajo pueden desaparecer en un instante, como resultado de un robo, un momento de descuido, la confiscación del hardware de la computadora, o simplemente debido a que la tecnología de almacenamiento es frágil por naturaleza. Existe un dicho común entre los profesionales dedicados al soporte técnico en el campo de la informática: "la cuestión no es *si* vas a perder tus datos; sino *cuando*." Por tanto, *cuando* esto te ocurra, es extremadamente importante que ya cuentes con un medio actualizado y probado de respaldo para poder restituir tus datos. Normalmente el día en que te recuerdan la importancia de un sistema de respaldo es al día siguiente que necesitaste tener uno en funcionamiento.

A pesar de ser uno de los elementos fundamentales de seguridad informática, el formular una política efectiva de mantenimiento de un respaldo no es tan simple como parece. Varios problemas se combinan para hacer de esto un obstáculo significativo, incluyendo la necesidad de almacenar datos originales y copias de seguridad o respaldos en diferentes ubicaciones físicas, la importancia de mantener confidenciales las copias de seguridad, y el reto de coordinar entre distintas personas quién comparte información con quién, utilizando sus propios dispositivos portátiles de almacenamiento. Además las copias de seguridad o respaldos y las tácticas de recuperación de archivos, este capítulo se ocupa de dos herramientas específicas, el *Cobian Backup* y el *Undelete Plus*.

Contexto

Elena es una activista ecológica en un país de habla rusa, donde ha comenzado a crear un sitio web que dependerá de la presentación creativa de imágenes, videos, mapas y relatos que hagan hincapié en el grado de deforestación ilegal en la región. Ella ha estado recolectando por años documentos, archivos de medios de comunicación e información geográfica sobre la tala de árboles, y la mayoría de ellos están almacenados en una vieja computadora que funciona con Windows en la oficina de la ONG donde ella trabaja. Mientras estaba diseñando un sitio web con relación a esta información, se dio cuenta de la importancia de ésta y se empezó a preocupar sobre su resguardo en caso de que su computadora sea dañada, especialmente si esto ocurre antes de tenga todo copiado al sitio web. Otros miembros de su organización a veces utilizan la computadora, de modo que ella desea saber cómo restituir sus archivos si alguien accidentalmente borra la carpeta que contiene su trabajo. Ella le pide a su sobrino Nikolai que la ayude a elaborar una estrategia vinculada a la creación y mantenimiento de una copia de seguridad o respaldo.

¿Qué aprenderás en este capitulo?

- Cómo organizar y hacer un respaldo de tu información
- Dónde debes almacenar tus respaldos o copias de seguridad
- Cómo debes administrar de manera segura tus respaldos
- Cómo recuperar archivos que han sido accidentalmente borrados

Identificar y organizar tu información

Aunque es evidentemente importante que des pasos para evitar desastres — asegurándote que tu información está físicamente a salvo, libre de *software malicioso (malware)* y protegido por un buen *cortafuegos (firewall)* y contraseñas sólidas — eso no es suficiente. Simplemente existen demasiadas cosas que pueden salir mal, incluyendo ataques virales, *piratas informáticos (hackers)*, cortos circuitos, picos de tensión eléctrica, derrames de agua, robo, confiscación, desmagnetización, problemas con el sistema operativo, fallas de hardware, para nombrar unos cuantos. El prepararse para el desastre es tan importante como defenderse de este.

Elena: Sé que un respaldo es importante, Nikolai, pero eso no significa que ¿Debería tener a alguien más que lo configure para mi? Es decir, ¿Tendré el tiempo, recursos y experiencia para hacer esto por mi cuenta?

Nikolai: No te preocupes. El desarrollar un buen plan de creación de respaldo requiere un poco de reflexión, pero no toma mucho tiempo ni dinero. Y, comparado con perder toda tu información, muy difícilmente podrías llamarlo inconveniente, ¿correcto? Aparte de ello, el respaldo es definitivamente una de esas cosas que debes hacer tu mismo. A menos que la persona que te ayuda regularmente en la parte técnica sea extremadamente confiable y esté extremadamente informada sobre donde mantienes tu información digital, lo mejor es configurar las cosas por ti mismo.

El primer paso para formular una política para el respaldo es imaginar donde se halla actualmente localizada tu información personal y laboral. Tu correo electrónico - por ejemplo - puede estar almacenado en el servidor del proveedor de correo electrónico, en tu propia computadora, o en ambos lugares al mismo tiempo. Y, por supuesto, puedes tener muchas cuentas de correo electrónico. Además, existen importantes documentos en las computadoras que utilizas, las cuales pueden estar en la oficina como en tu domicilio. Hay agendas de direcciones, el historial de conversaciones y configuraciones personales de programas. También es posible que alguna información sea también almacenada en medios removibles, como memorias extraíbles USB, discos duros externos, CDs, DVDs, y viejos disquetes. Tu teléfono móvil tiene una lista de contactos y podría tener importantes mensajes de texto. Si tienes un sitio web, este podría contener una gran colección de artículos acumulados a lo largo de años de trabajo. Y, finalmente, no te olvides de tu información que no se halla en medios digitales, tales como agendas físicas, diarios y cartas.

Luego, necesitas definir cuales de estos archivos son 'copias maestras', y cuales son duplicados. La copia maestra es generalmente la versión más actualizada de un archivo en particular o una colección de archivos y corresponde a un archivo que en realidad editarás si necesitas actualizar su contenido. Obviamente esta

distinción no se aplica a archivos de los cuales tienes una única copia, pero es extremadamente importante para ciertos tipos de información. Una situación común de desastre es cuando sólo los duplicados de cada documento importante son respaldados, y la copia maestra en sí se perdió o destruyó antes que estos duplicados pudieran ser actualizados. Imagina, por ejemplo, que has estado trabajando por una semana mientras actualizabas la copia de determinada hoja de cálculo que mantienes en tu memoria extraíble USB. A estas alturas, deberías empezar a pensar en aquella como tu copia maestra, debido a que los respaldos de la versión desactualizada que se hallan en la computadora de la oficina ya no son útiles.

Trata de anotar la ubicación física de todas tus copias maestras y de los duplicados de la información identificada anteriormente. Ello te ayudará a aclarar tus necesidades y empezar a definir una adecuada política de respaldos o copias de seguridad. El cuadro que hallamos a continuación es un ejemplo muy básico. Por supuesto, tu probablemente te percates que tu lista es mucho más extensa, y contiene algunos 'dispositivos de almacenamiento' con más de un 'tipo de dato' y algunos tipos de datos que se encuentran presentes en múltiples dispositivos.

Tipo de Datos	**Copia Maestra/Duplicado**	**Dispositivo de Almacenamiento**	**Ubicación**
Documentos electrónicos	Copia Maestra	Disco duro de la computadora	Oficina
Unos cuantos documentos electrónicos importantes	Duplicado	Memoria extraíble USB	Conmigo
Bases de datos de aplicaciones (fotos, agenda de direcciones, calendario, etc.)	Copia Maestra	Disco duro de la computadora	Oficina
Unos cuantos documentos electrónicos	Duplicado	CDs	Domicilio
Correo electrónico & contactos de correo electrónico	Copia Maestra	Cuenta de Gmail	Internet
Mensajes de texto & contactos telefónicos	Copia Maestra	Teléfono móvil	Conmigo
Documentos impresos (contratos, facturas, etc.)	Copia Maestra	Cajón de escritorio	Oficina

En el cuadro anterior, puedes apreciar que:

- Los únicos documentos que sobrevivirían si falla el disco duro de tu computadora de tu oficina son los duplicados en tu memoria extraíble USB y las copias en CD en tu domicilio.
- No tienes copias de tus mensajes de correo electrónico sin conexión o de tu agenda, de modo que si olvidas tu contraseña (o si alguien logra cambiarla maliciosamente), perderás acceso a ella.
- No tienes copias de ningún dato de tu teléfono móvil.
- No tienes duplicados, digitales o físicos, de documentos impresos tales como contratos y facturas.

Definir una estrategia para tu respaldo

Para hacer el respaldo de todos los datos listados anteriormente necesitarás una combinación de software y soluciones de proceso. Esencialmente debes asegurarte que cada tipo de datos sea almacenado en al menos dos lugares separados.

Documentos electrónicos - Crea el respaldo completo de todos los documentos en tu computadora utilizando un programa como el *Cobian Backup*, el cual se detalla más adelante. Almacena el respaldo en algún dispositivo portátil de modo que puedas llevarlo a tu domicilio o a cualquier otro lugar seguro. Puede ser más fácil utilizar CDs o DVDs para ello, en vez de en un disco duro externo o una memoria extraíble USB, de modo que no corras el riesgo de perder tus viejos respaldos mientras estas transportando uno nuevo. Los CDs en blanco pueden ser lo suficientemente baratos de modo que puedas utilizar uno nuevo cada vez que hagas un respaldo. Debido a que este tipo de datos a menudo contienen la información más sensible, es particularmente importante que protejas los respaldos de tus documentos electrónicos utilizando un tipo de cifrado. Puedes aprender como hacerlo en el capítulo **4. Proteger los archivos sensibles en tu computadora** y en la **guía del TrueCrypt**.

Bases de datos de aplicaciones - Una vez que hayas determinado la ubicación de tus bases de datos de aplicaciones, puedes respaldarlas en la misma forma que con los documentos electrónicos.

Correo electrónico - En vez de ingresar a tu correo electrónico sólo a través de un navegador web, instala un cliente de correo electrónico como el *Thunderbird* y configúralo para funcionar con tu cuenta. La mayoría de los servicios de correo con interfaz web te proporcionarán instrucciones de cómo utilizar dichos programas y - a menudo - cómo importar tu dirección de correo electrónico a este. Puedes aprender más sobre esto en la sección Lecturas Adicionales que viene más adelante. Asegúrate de dejar una copia de tus mensajes en el servidor de correo, en vez de sólo desplazarlos a tu computadora. La **guía del Thunderbird** te explica en detalle cómo hacerlo.

Contenidos de teléfono móvil - Para hacer un respaldo de los números telefónicos y mensajes de texto en tu teléfono móvil, puedes conectarlo a la computadora utilizando el software apropiado, el cual está normalmente disponible en el sitio web del fabricante de tu teléfono. Sin embargo, para esto puedes necesitar comprar un cable especial USB. Como alternativa, puedes utilizar el teléfono para copiar tus mensajes de texto e información de contactos de tu *tarjeta SIM* en el teléfono mismo, y luego copiarlos en una tarjeta SIM de respaldo. Este método puede ser muy útil como una solución de emergencia para crear un respaldo, pero recuerda mantener a salvo la tarjeta SIM adicional. La capacidad de copiar la información de contacto y los mensajes de texto entre un teléfono móvil y su tarjeta SIM es una característica estándar, pero si tu teléfono permite almacenar este tipo de información en una tarjeta de memoria extraíble, entonces el proceso de respaldo puede ser incluso más fácil.

Documentos impresos - Cuando sea posible, debes escanear todos tus documentos importantes, luego respaldarlos junto con otros documentos electrónicos, de la manera como se expone anteriormente.

Al final debes haber dispuesto de manera diferente tus dispositivos de almacenamiento, tipos de datos y respaldos de manera que tu información sea más resistente al desastre:

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Documentos electrónicos	Copia Maestra	Disco duro de la computadora	Oficina
Documentos electrónicos	Duplicado	CDs	Domicilio
Unos cuantos documentos electrónicos importantes	Duplicado	Memoria extraíble USB	Conmigo

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Bases de datos de aplicaciones	Copia Maestra	Disco duro de la computadora	Oficina
Bases de datos de aplicaciones	Duplicado	CDs	Domicilio

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Correo electrónico & contactos de correo electrónico	Duplicado	Cuenta Gmail	Internet
Correo electrónico & contactos de correo electrónico	Copia Maestra	Thunderbird en la computadora de la oficina	Oficina

Tipo de Datos	Copia Maestra/Duplicado	Dispositivo de Almacenamiento	Ubicación
Mensajes de texto & contactos en el teléfono móvil	Copia Maestra	Teléfono móvil	Conmigo

Mensajes de texto & contactos en el teléfono móvil	Duplicado	Disco duro de la computadora	Oficina
Mensajes de texto & contactos en el teléfono móvil	Duplicado	Tarjeta SIM de respaldo	Domicilio

Tipo de Datos	**Copia Maestra/Duplicado**	**Dispositivo de Almacenamiento**	**Ubicación**
Documentos impresos	Copia Maestra	Cajón de escritorio	Oficina
Documentos escaneados	Duplicado	CDs	En casa

Elena: Sé de personas que guardan todos sus documentos importantes en Gmail, adjuntándolos a mensajes del tipo 'borrador' o inclusive a correos electrónicos. ¿Ello podría considerarse como una 'ubicación física secundaria' para mis archivos?

Nikolai: Te podría ayudar a recuperarlos si pierdes uno o dos documentos muy importantes, pero es muy comprometedor. Sinceramente, ¿cuántos documentos por semana estarías dispuesto a respaldar de esa forma? Además, debes considerar si dichos archivos adjuntos están seguros o no, especialmente si estás preocupada sobre si tu correo electrónico está siendo vigilado. A menos que estés conectada de manera segura al Gmail, esto es como entregar tu información sensible en una bandeja de plata. El utilizar una conexión HTTPS para Gmail con el fin de respaldar pequeños volúmenes de TrueCrypt o archivos de bases de datos de KeePass sería muy seguro, debido a que estos se hallan cifrados, pero yo no te recomendaría esto como una estrategia de respaldo de propósito general.

Crear un respaldo digital

De los distintos tipos de datos aludidos aquí, es de los 'documentos electrónicos' de los que las personas tienden a preocuparse más cuando establecen una política de respaldo. Este término es algo ambiguo, pero generalmente se refiere a archivos de los cuales estás al tanto y que abres manualmente ya sea a través de una doble pulsación con el ratón o utilizando la función Archivo del menú en una aplicación particular. Específicamente, el término incluye archivos de texto, documentos de procesador de textos, presentaciones, PDFs y hojas de cálculo, entre otros ejemplos. A diferencia de los mensajes de correo electrónico, por ejemplo, los documentos electrónicos generalmente no están sincronizados con copias remotas en la Internet.

Cuando hagas el respaldo de tus documentos electrónicos debes recordar también respaldar las bases de datos de tus aplicaciones. Si utilizas una aplicación de calendario o una agenda electrónica, por ejemplo, necesitarás encontrar la carpeta en las cuales estos programas almacenan sus datos. Felizmente, estas bases de datos estarán en la misma ubicación de tus documentos electrónicos, ya que a menudo se mantienen dentro de la carpeta *Mis Documentos* en una computadora con Windows. Sin embargo, si ese no es el caso, debes añadir las carpetas pertinentes a tu respaldo normal.

Los correos electrónicos almacenados por una aplicación tal como el Mozilla *Thunderbird* es un ejemplo especial de un base de datos de aplicación. Si utilizas un programa de correo electrónico — y especialmente si eres incapaz o no deseas almacenar una copia de tus mensajes en el servidor — entonces debes de todas maneras asegurarte que esta base de datos de correo electrónico se incluya en tu respaldo normal. Puedes considerar a las imágenes y archivos de video como documentos electrónicos o elementos dentro de una base de datos de aplicación, eso depende de cómo interactúas con ellos. Las aplicaciones tales como el Windows Media Player y el iTunes, por ejemplo, funcionan como bases de datos. Si utilizas programas como estos, debes buscar en tu disco duro para saber donde se almacenan los archivos multimedia existentes que estos te ayudan a administrar.

Dispositivos de almacenamiento

Antes de hacer un respaldo de tus documentos electrónicos, debes decidir que tipo de dispositivo de

almacenamiento usarás.

Discos Compactos (CDs) - Los CDs almacenan alrededor de 700 Megabytes (MB) de datos. Para crear un respaldo en CD necesitarás un *quemador de CD* y discos en blanco. Si deseas borrar un CD y actualizar los archivos almacenados en este, necesitarás tener un quemador de CD-RW y CDs regrabables. Todos los más difundidos sistemas operativos, incluyendo el Windows XP, ahora incluyen un software que puede grabar CDs y CD-RWs. Ten en cuenta que la información escrita en estos discos puede empezar a deteriorarse después de cinco o diez años. Si necesitas almacenar un respaldo por un tiempo mayor a estos, tendrás que recrear alguna vez los CDs, comprar discos especiales de 'larga vida' o utilizar un método diferente de respaldo.

Discos Digitales de Video (DVDs) - Los DVDs almacenan hasta 4.7 Gigabytes (GB) de datos. Funcionan en forma parecida a los CDs pero necesitan un equipo ligeramente más costoso. Necesitarás un quemador de DVD o un *quemador de DVD-RW*, y discos apropiados. Del mismo modo como los CD, los datos escritos en un DVD normal finalmente empezarán a desaparecer.

Memorias extraíbles USB - Una memoria extraíble USB almacena tanta información como su capacidad lo permita. Las memorias extraíbles USB pueden ser muy costosas, incluso aquellas con una capacidad igual o mayor que la de un CD o DVD, y son fáciles de borrar o regrabar numerosas veces. Como los CDs y DVDs, las memorias extraíbles USB tienen un tiempo de vida limitado, el cual se estima generalmente en alrededor de 10 años.

Servidor remoto - Un bien mantenido servidor de red de respaldo puede tener una capacidad casi ilimitada, pero la velocidad y la estabilidad de tu propia conexión de Internet determinará si esta es o no una opción realista. Ten en consideración que hacer un respaldo en un servidor en tu propia oficina, aunque más rápido que copiar información en la Internet, viola el requerimiento de mantener una copia de tus datos importantes en dos lugares físicos diferentes. Existen también servicios de almacenamiento gratuito en la Internet, pero siempre debes cifrar tus respaldos antes de subirlos a servidores a cargo de organizaciones o individuos a quiénes no conoces ni en quiénes confias. Dirígete a la sección **Lecturas Adicionales** para ver algunos ejemplos.

Software para hacer respaldos

El *Cobian Backup* es una herramienta de fácil manejo que puede configurarse para funcionar automáticamente, en periodos predeterminados, y para incluir solo los archivos que han sido modificados desde la última creación de respaldo. Este también puede comprimir respaldos para hacerlos más pequeños.

Como siempre, es una Buena idea cifrar tus archivos de respaldo utilizando una herramienta como el *TrueCrypt*. Más información sobre el cifrado de datos puede hallarse en el capítulo **4. Proteger los archivos sensibles en tu computadora**.

Cuando estés utilizando estas herramientas para hacer respaldos, hay algunas cosas que puedes hacer para ayudar a que tu sistema de hacer respaldos funcione sin problemas:

- Organiza los archivos en tu computadora. Trata de trasladar todas las carpetas que contienen documentos electrónicos que intentas respaldar a un solo lugar, tal como la carpeta **Mis Documentos**.
- Si utilizas un software que almacena sus datos en una base de datos de aplicación, debes primero determinar la ubicación de dicha base de datos. Si no está en un lugar conveniente, infórmate si el programa te permite elegir una nueva ubicación para su base de datos. Si es posible, puedes colocar esta en la misma carpeta de tus documentos electrónicos.
- Crea un cronograma regular para hacer tu respaldo.
- Trata de establecer procedimientos para todo el personal en tu oficina que todavia no tiene una política confiable y segura de respaldos. Ayuda a tus compañeros de trabajo a entender la importancia de este tema.
- Asegúrate de probar el proceso de recuperación de datos de tu respaldo o copia de seguridad. Recuerda, que al final, ¡es el proceso de restitución — no el procedimiento de respaldo — el que de veras te importa!

Elena: Está bien, por ello hice un respaldo cifrado mientras estaba en el trabajo, y lo grabé en un CD. El Cobian está programado para actualizar mi respaldo en unos cuantos días. Mi escritorio en el trabajo tiene un cajón con cerradura, y estoy pensando mantener los CDs de respaldo en este de modo que no se pierdan o

rompan.

Nikolai: ¿Qué sucedería si tu oficina se incendia? ¿La computadora, el escritorio, los CDs de respaldo y todo lo demás? O, ¿Qué ocurriría si tu sitio web es utilizado para planificar una demostración medioambiental gigante, las autoridades los combaten, las cosas se van de las manos, y la organización es intervenida? Dudo mucho que tu pequeño escritorio detenga a la policía de confiscar esos CDs. ¿Por qué no tenerlos en casa, o pedir a un amigo que los guarde por ti?

Recuperarse de un borrado accidental de archivos

Cuando borras un archivo en Windows, este desaparece de la vista, pero sus contenidos se mantienen en la computadora. Incluso después de que hayas vaciado tu Papelera de Reciclaje, la información de los archivos que has borrado pueden normalmente ser ubicados en el disco duro. Dirígete al capítulo **6. Destruir información sensible** para aprender más sobre esto. De vez en cuando, si accidentalmente borras un archivo o carpeta importante, esta vulnerabilidad de seguridad puede trabajar a tu favor. Existen numerosos programas que pueden restituir el acceso a tus recientemente borrados archivos, incluyendo un herramienta de *Software Libre y de Código Abierto (FOSS)* llamada *Undelete Plus*.

Estas herramientas no siempre funcionan, debido a que Windows pudo haber escrito nuevos datos sobre tu información borrada. Por tanto es importante que utilices lo menos posible tu computadora en el tiempo entre el borrado del archivo y el intento de restituirlo con una herramienta como *Undelete Plus*. Cuanto más tiempo utilices tu computadora antes de intentar restituir el archivo, será menos probable que tengas éxito. Esto también significa que debes instalar el software de recuperación de datos con mucha anticipación. Si tienes que instalarlo después de que has borrado un archivo importante, existe la posibilidad de que el software mismo se escriba sobre los datos indispensables que estás tratando de recuperar.

Aunque puede parecer mucho trabajo el implementar las políticas y aprender a utilizar las herramientas descritas en este capítulo, el mantener tu estrategia de respaldo, una vez que tengas un sistema en pie, es mucho más fácil que configurarla por primera vez. Y dado que el respaldo puede ser el aspecto individual más importante de la seguridad de datos, puedes estar seguro que el esfuerzo de recorrer todo el proceso bien vale la pena.

6. Destruir información sensible

Los capítulos anteriores se han ocupado de varias herramientas y hábitos que pueden ayudarte a proteger tus datos sensibles, pero ¿Qué ocurre cuando decides que ya no necesitas más conservar una parte de tu información? Si determinas, por ejemplo, que tus copias cifradas de respaldo de un archivo en particular son suficientes, y deseas borrar la copia maestra, ¿Cuál es la mejor forma de hacerlo? Lamentablemente, la respuesta es más complicada de lo que crees. Cuando borras un archivo, incluso antes de vaciar la **Papelera de Reciclaje**, los contenidos de dicho archivo se mantienen en tu disco duro y pueden ser recuperados por cualquiera que tenga un poco de suerte y las herramientas adecuadas.

Con el fin de garantizar que la información borrada no termine en las manos equivocadas tendrás que confiar en un software especial que remueva los datos de manera segura y permanente. El *Eraser* es una de tales herramientas, y se abordará más adelante. Utilizar el Eraser es un poco como hacer trizas un documento de papel en vez de simplemente arrojarlo dentro de una papelera y esperar que nadie lo encuentre. Y, por supuesto, el borrar archivos es solo un ejemplo de una situación en la cual podrías necesitar destruir datos sensibles. Si consideras los detalles que alguien, particularmente un adversario poderoso y motivado políticamente, podría descubrir sobre ti o tu organización al leer ciertos archivos que pensaste que habías borrado, podrías probablemente pensar en algunos cuantos ejemplos más: destruir respaldos obsoletos, *eliminar permanentemente* los datos de viejos disco duros antes de regalarlos, borrar viejas cuentas de usuario, y limpiar tu historial de navegación, para mencionar unos cuantos. La otra herramienta descrita en este capitulo es el *CCleaner*, que te puede ayudar a afrontar el reto de borrar los muchos archivos temporales que tu sistema operativo y las aplicaciones crean cada vez que los usas.

Contexto

Elena es una activista medioambiental en un país de habla rusa, donde mantiene un crecientemente popular sitio web que hace hincapié en la magnitud de la deforestación ilegal en la región. Ella ha creado un respaldo de la información utilizada para crear el sitio web, y mantiene copias de este en casa, en la oficina y en su nueva computadora portátil. Hace poco, ha empezado a almacenar copias de los registros de visita de los servidores web y de la base de datos que contiene sus mensajes en el foro de usuarios. Elena pronto hará un viaje internacional, para asistir a una gran conferencia mundial de activistas medioambientales, algunos de los cuales han informado que sus computadoras portátiles les fueron quitadas por aproximadamente una hora en los pasos fronterizos. Para proteger su información sensible, y la seguridad de los participantes más políticos de su foro, ella ha trasladado sus respaldos de casa y de la oficina a un volumen TrueCrypt y ha removido la copia que había en su computadora portátil. Le pidió consejo a su sobrino Nikolai, y él le advirtió que tiene que hacer algo más que sólo borrar su viejo respaldo si le preocupa la retención de su computadora a cargo de los funcionarios de fronteras.

¿Qué puedes aprender de este capítulo?

- Eliminar de manera permanente información sensible de tu computadora
- Eliminar información almacenada en tus dispositivos de almacenamiento removibles tales como CDs y memorias extraíbles USB
- Evitar que alguien sepa que documentos has estado viendo previamente en tu computadora
- Mantener tu computadora de modo que los archivos borrados no puedan ser recuperados en el futuro

Borrar información

Desde una perspectiva puramente técnica no existe en tu computadora una función de borrado propiamente dicha. Por supuesto puedes arrastrar un archivo a la **Papelera de Reciclaje** y vaciarla, pero todo esto en realidad simplemente borra el icono, elimina el nombre del archivo de una especie de índice de todo el contenido en tu computadora y le dice a Windows que puede utilizar ese espacio para algo más. Sin embargo, hasta que esto ocurra dicho espacio será ocupado por los contenidos de la información borrada, algo muy parecido a un gabinete de archivos al que se le ha sacado todas sus etiquetas pero todavía contiene todos los archivos originales. Es por esto que si cuentas con el software adecuado y actúas con prisa, puedes recuperar la información que borraste por accidente, como se trató en el capítulo **5. Recuperar información perdida**.

Debes tener en cuenta que cada vez que usas tu computadora, se crean archivos y estos mismos son borrados de manera insegura, sin tu conocimiento. Supón, por ejemplo, que estás escribiendo un informe extenso. Este te podría tomar una semana, trabajando muchas horas a diario, y cada vez que el documento es guardado, Windows creará una nueva copia del documento y lo almacenará en tu disco duro. Después de unos cuantos días de editado, tú puedes sin saberlo haber guardado muchas versiones del documento, todas en diferentes etapas de avance.

Por supuesto, Windows generalmente borra las versiones antiguas de un archivo, pero no busca la ubicación exacta del original para sobrescribirlo de manera segura cuando se hace una nueva copia. En vez de ello, este simplemente pone la última versión en una nueva sección del hipotético gabinete de archivos mencionado anteriormente, es decir, traslada la etiqueta de la vieja sección a la nueva, y deja el anterior borrador donde estaba hasta que otro programa requiera utilizar ese espacio. Está claro, que si tú tienes una buena razón para destruir todos los rastros de dicho documento de tu gabinete de archivos, el borrar la última copia no será suficiente, y simplemente el botar la etiqueta sería mucho peor.

También debes recordar, que los discos duros de la computadora no son los únicos dispositivos que almacenan información digital. Los CDs, DVDs., las memorias extraíbles USB, los disquetes, las tarjetas de memoria flash de los teléfonos móviles y los discos duros externos tienen los mismos problemas, y no debes confiar simplemente en una simple operación de borrar o reescribir para desaparecer información sensible de cualquiera de ellos.

Eliminar permanentemente información con herramientas seguras de borrado

Cuando utilizas una herramienta de borrado seguro - tal como aquellas recomendadas en este capitulo - sería más preciso decir que estás reemplazando, o 'sobrescribiendo', tu información sensible, en vez de simplemente borrarla. Si imaginas que dichos documentos, en el gabinete de archivos deficientemente etiquetado que mencionamos antes, están escritos a lápiz, entonces un software de borrado seguro no sólo borra el contenido, sino que garabatea sobre cada palabra. Y - en forma muy parecida al trazo de la mina de un lápiz - la información digital puede todavía leerse, aunque con dificultad, incluso después de que ha sido borrada y se ha escrito algo sobre ella. Debido a esto las herramientas recomendadas aquí sobrescriben archivos múltiples veces con datos aleatorios. A este proceso se le llama *eliminar permanentemente*, y cuantas más veces es sobrescrita la información, mayor es la dificultad para que alguien pueda recuperar el contenido original. Los expertos coinciden generalmente que tres o más pasadas deben hacerse — algunos estándares recomiendan siete o más — pero el software de eliminación permanente de datos se ocupa de esto automáticamente.

Eliminar permanentemente archivos

Existen dos maneras comunes de *eliminar permanentemente* datos sensibles de tu disco duro o de tu dispositivo de almacenamiento. Puedes eliminar permanentemente un archivo o puedes eliminar permanentemente todo el espacio 'no asignado' en la unidad. Cuando tomes esta decisión, puede ser útil considerar nuestro ejemplo previo del extenso informe que haya podido dejar copias incompletas esparcidas en todo tu disco duro aunque sólo un archivo es visible. Si eliminas permanentemente el archivo mismo, garantizas que la actual versión esta completamente removida, pero dejas las otras copias donde esten. De hecho, no existe manera de apuntar directamente a dichas copias, debido a que ellas no están visibles sin utilizar un software especial. Sin embargo, al eliminar permanentemente todo el espacio en blanco de tu dispositivo de almacenamiento, te aseguras que toda la información anteriormente borrada sea destruida. Regresando a la metáfora del gabinete de archivos, este procedimiento es comparable a buscar en el gabinete, borrar y garabatear sobre cada documento cuya etiqueta haya sido retirada.

El *Eraser* es una herramienta de borrado segura, libre y de código abierto, que es extremadamente fácil de usar. Con el Eraser puedes *eliminar permanentemente* archivos en tres diferentes formas: seleccionando un solo archivo, seleccionando el contenido de la **Papelera de Reciclaje**, o eliminando permanentemente todo el espacio no asignado en la unidad. El Eraser puede también eliminar permanentemente los contenidos del *archivo de paginación o intercambio* de Windows, como se abordó anteriormente.

Aunque las herramientas de borrado seguro no dañarán ningún archivo visible a menos que tú expresamente los elimines permanentemente, es importante ser cuidadoso con un software como este. Después de todo los accidentes ocurren, es por ello que la gente considera muy útiles a la **Papelera de Reciclaje** y a las herramientas de recuperación de datos. Si te acostumbras a *eliminar permanentemente* tus datos cada vez que borras algo, te encontraras sin forma de recuperarte de un simple error. Asegúrate siempre de tener un respaldo seguro antes de eliminar permanentemente grandes cantidades de datos de tu computadora.

Elena: Sé que los programas de procesamiento de textos como Microsoft Word y Open Office a veces realizan copias temporales de archivos mientras estás trabajando en ellos. Existen otros programas que hagan lo mismo, o ¿debo solamente preocuparme en mayor parte sobre los archivos que yo he creado y borrado?

Nikolai: En realidad, existen muchos lugares en tu computadora donde los programas dejan rastros de tu información personal y de tus actividades en línea. Te hablo de los sitios web que has visitado, los borradores de correos electrónicos que has escrito recientemente y otras cosas parecidas. Todo esto podría ser sensible, dependiendo de cuan a menudo utilizas esa computadora.

Eliminar permanentemente datos temporales

La opción que permite al *Eraser* *eliminar permanentemente* todo el espacio no asignado de una unidad no es tan riesgoso como parece, debido a que sólo elimina permanentemente contenido borrado anteriormente. Los archivos visibles normalmente no serán afectados. Por otro lado, este mismo hecho sirve para resaltar un

aspecto diferente: el Eraser no puede ayudarte a limpiar la información sensible que no ha sido borrada pero que pudiera estar extremadamente bien oculta. Los archivos que contienen dichos datos pueden estar metidos en carpetas oscuras, por ejemplo, o almacenados con nombres sin significado. Este no es un gran problema para documentos electrónicos, pero puede ser importante para información que se recolecta automáticamente cada vez que utilizas tu computadora. Ejemplos de ello incluyen:

- Datos temporales registrados por tu navegador mientras te muestra páginas web, incluyendo texto, imágenes, *cookies*, información de cuenta, datos personales utilizados para llenar formularios en línea y el historial de sitios web visitados.
- Archivos temporales guardados por varias aplicaciones con el fin de ayudarte a recobrarlos en caso se cuelgue tu computadora antes de que guardes tu trabajo. Estos archivos pueden contener texto, imágenes, datos de hojas de cálculo y los nombres de otros archivos, entre otra información potencialmente sensible.
- Archivos y enlaces almacenados por Windows en nombre de la conveniencia, tales como accesos directos a aplicaciones que has utilizado recientemente, enlaces obvios a carpetas que preferirías ocultas y, por supuesto, los contenidos de tu **Papelera de Reciclaje** que olvidaste vaciar.
- El *archivo de paginación o de intercambio* de Windows. Cuando la memoria de tu computadora está llena, como cuando has estado ejecutando muchos programas al mismo tiempo en una vieja computadora, Windows a veces copia los datos que estás utilizando en un archivo extenso llamado archivo de paginación o de intercambio. Como resultado de ello este archivo puede contener casi todo, incluyendo las páginas web, los contenidos de los documentos, las contraseñas o las claves de cifrado. Incluso cuando apagas tu computadora, el archivo de paginación o intercambio no se remueve, por ello debes *eliminarlo permanentemente* de forma manual.

Con el fin de remover archivos temporales comunes de tu computadora, puedes utilizar la herramienta de software libre llamada *CCleaner*, la cual fue diseñada para realizar la limpieza después de utilizar programas como el Internet Explorer, Mozilla *Firefox* y las aplicaciones de Microsoft Office — todas las cuales son conocidas por exponer información potencialmente sensible — así como el mismo Windows. El CCleaner puede borrar archivos de forma segura, lo cual te ahorra el tener que *eliminar permanentemente* el espacio no asignado de la unidad, usando el *Eraser*, después de utilizarlo.

Consejos para utilizar de manera efectiva las herramientas seguras de borrado

Ahora que estás familiarizado con algunas de las formas en las cuales la información puede ser expuesta en tu computadora o en un dispositivo de almacenamiento, incluso si eres diligente en cuanto al borrado de archivos sensibles. También sabes que herramientas puedes utilizar para *eliminar permanentemente* dicha información en forma permanente. Existen unos cuantos pasos simples que debes seguir, especialmente si es la primera vez que estás utilizando estas herramientas, con el fin de garantizar que tu unidad sea limpiada de manera segura y efectiva:

- Crea un respaldo cifrado de tus archivos más importantes, como se trató en el capítulo **5. Recuperar información perdida**.
- Cierra todos los programas innecesarios y desconéctate de Internet.
- Borra todos los archivos innecesarios, de todos los dispositivos de almacenamiento, y vacía la *Papelera de Reciclaje*.
- *Elimina permanentemente* los archivos temporales utilizando el *CCleaner*.
- Elimina permanentemente el *archivo de paginación o de intercambio* de Windows utilizando el *Eraser*.
- Elimina permanentemente todo el espacio libre de tu computadora y de otros dispositivos de almacenamiento utilizando el Eraser. Podrías necesitar que este procedimiento se ejecute en la noche, pues puede ser muy lento.

Luego, debes habituarte a:

- Utilizar periódicamente el *CCleaner* para *eliminar permanentemente* tus archivos temporales

- *Eliminar permanentemente* los documentos electrónicos sensibles utilizando el *Eraser*, en vez de utilizar la *Papelera de Reciclaje* o la función de borrado de Windows
- Utilizar periódicamente el Eraser para eliminar permanentemente el archivo de paginación o de intercambio de Windows
- Utilizar periódicamente el Eraser para eliminar permanentemente todo el espacio no asignado en tus discos duros, memorias extraíbles USB, y cualquier otro dispositivo de almacenamiento que pudiera tener información sensible borrada recientemente. Entre ellos se puede incluir disquetes, CDs regrabables, DVDs regrabables y tarjetas de memoria flash de cámaras, teléfonos móviles o reproductores portátiles de música.

Consejos para eliminar permanentemente el contenido completo de un dispositivo de almacenamiento

Podrías ocasionalmente necesitar *eliminar permanentemente* los contenidos de un dispositivo de almacenamiento. Cuando vendes o regalas una vieja computadora, lo mejor es retirar el disco duro y que el nuevo dueño de la computadora adquiera una para sí. Sin embargo, si esta no es una opción, debes al menos eliminar permanentemente los contenidos del disco de manera rigurosa con el *Eraser* antes de entregarlo. Incluso en el caso en el que conserves el disco, probablemente quieras eliminar permanentemente de todas maneras su contenido, sin importar si pretendes reutilizarlo o desecharlo. De manera similar si compras un nuevo disco duro, debes eliminar permanentemente los contenidos del antiguo después de copiar tus datos y hacer un respaldo seguro de este. Si lo que pretendes es botar o reciclar un viejo disco duro, también debes considerar el destruirlo físicamente. (Muchos profesionales a cargo del mantenimiento de las computadoras recomiendan unos cuantos golpes fuertes con un martillo antes de desechar cualquier dispositivo de almacenamiento que alguna vez contuvo información sensible.)

En cualquiera de las situaciones descritas anteriormente, necesitarás utilizar el *Eraser* para *eliminar permanentemente* el contenido total de un disco duro, lo cual es imposible mientras el sistema operativo se este ejecutando en ese disco en particular. La manera más fácil de tratar este asunto es remover el disco y colocarlo en una 'cubierta de disco' externa USB la cual puedes luego conectar a cualquier computadora que tenga instalado el Eraser. En este punto, puedes borrar el contenido completo del disco externo y luego utilizar el Eraser para eliminar permanentemente todo su espacio no asignado. Afortunadamente, esto no es algo que tengas que hacer a menudo, pues puede tomar un buen periodo de tiempo.

En vez de *eliminar permanentemente* los datos que han sido almacenados en un CD o DVD regrabable, es mejor destruir el disco mismo. Si es necesario, puedes crear uno nuevo que contenga cualquier información que desees mantener. Y, por supuesto, esta es la única manera de 'borrar' el contenido de un disco no regrabable. Es sorprendentemente difícil destruir completamente los contenidos de un CD o DVD. Seguramente has escuchado historias sobre información recuperada de tales discos incluso después de que fueran cortados en pequeños pedazos. Aunque estas historias son ciertas, el reconstruir la información de esta manera toma mucho tiempo y pericia. Debes juzgar por ti mismo si es probable o no que alguien gaste ese nivel de recursos con el fin de acceder a tus datos. Normalmente, un par de fuertes tijeras o una fuerte cortadora de papel hará un buen trabajo. Si deseas tomar precauciones adicionales, puedes mezclar las piezas resultantes y disponer de ellas en varias ubicaciones alejadas de tu casa u oficina.

Elena: Todavía tengo un viejo CD de respaldo de los registros del servidor web, y escuché que puedes borrar un CD colocándolo en el microondas. Sin embargo, esto me suena a una mala idea. ¿Las personas en realidad hacen esto? ¿Realmente funciona?

Nikolai: Me imagino que destruye los datos de manera muy efectiva, pero no podría saberlo, porque ¡nunca pondría un CD en un microondas! Estás en lo correcto. Eso suena como una muy mala idea. Incluso si el metal no daña tu microondas o inicia un incendio, te apuesto que el plástico emitirá humos muy insalubres. Pensando en ello, no recomendaría tampoco el someter CDs al fuego.

7. Mantener privada tu comunicación en Internet

La conveniencia, la relación costo-beneficio y la flexibilidad del correo electrónico y de la mensajería instantánea los hace extremadamente valiosos para las personas y las organizaciones, incluso para aquellas con el acceso más limitado a la Internet. Para aquellos con conexiones más rápidas y más confiables, programas como *Skype* y otras herramientas de *Voz sobre Protocolo de Internet (VoIP)* también comparten estas características. Lamentablemente, estas alternativas digitales a los medios tradicionales de comunicación no siempre pueden ser confiables para mantener privada información sensible. Por supuesto, esto no es nada nuevo. El correo postal, las llamadas telefónicas y los mensajes de texto también son todos vulnerables, particularmente cuando se utilizan por y quienes son objeto de vigilancia por parte de las autoridades.

Una diferencia importante entre las comunicaciones digitales, métodos de comunicación basados en Internet y métodos más tradicionales, es que la primera a menudo te permite elegir tu propio nivel de seguridad. Si envías correos electrónicos, mensajes instantáneos y conversaciones en *Voz sobre Protocolo de Internet (VoIP)* utilizando métodos inseguros, estos son casi con certeza menos privados que las cartas físicas o las llamadas telefónicas. Esto ocurre, en parte, debido a que algunas muy poderosas computadoras pueden automáticamente buscar a través de grandes cantidades de información digital para identificar a los remitentes, los destinatarios y palabras claves específicas. Se requieren de grandes recursos para llevar a cabo el mismo nivel de vigilancia para canales de comunicación tradicionales. Sin embargo, si tomas ciertas precauciones, puedes hacer realidad lo opuesto. La flexibilidad de las herramientas de comunicación de Internet y la fortaleza del *cifrado* moderno pueden ahora proporcionarnos un nivel de privacidad que alguna vez sólo estuvo al alcance de los ejércitos nacionales y de las organizaciones de inteligencia.

El seguir las guías y explorar el software que se trata en este capítulo, te ayudará a mejorar enormemente la seguridad de tus comunicaciones. El servicios de correo electrónico *Riseup*, el complemento *OTR* para el programa de mensajería instantánea de *Pidgin*, el Mozilla *Firefox* y el complemento *Enigmail* para el cliente de correo electrónico Mozilla *Thunderbird* son todas excelentes herramientas. Sin embargo, cuando las utilices debes tener en cuenta que la privacidad de una conversación dada nunca está cien por ciento garantizada. Siempre existe alguna amenaza que no has considerado, ya sea un *registrador de teclas (keylogger)* en tu computadora, una persona escuchando tras la puerta, un corresponsal de correo electrónico descuidado o algo completamente diferente. El objetivo de este capítulo es ayudarte a reducir, en lo posible, dichas amenazas. No es el de hacerte olvidar que existen ni para defender la posición extrema, favorecida por algunos, de que nada que no harías publico con gusto, debe enviarse por Internet.

Contexto

Claudia y Pablo trabajan con una ONG de derechos humanos en un país sudamericano. Después de pasar varios meses recolectando testimonios de testigos de violaciones de derechos humanos que fueron cometidos por miembros del ejército en su región, Claudia y Pablo han empezado a dar pasos para proteger los datos resultantes. Ellos mantienen sólo la información que necesitan, la cual almacenan en una partición TrueCrypt que está respaldada en varias ubicaciones físicas. Mientras se preparan para publicar ciertos aspectos de estos testimonios en un próximo informe, ellos se han percatado que deben debatir información sensible con unos cuantos de sus colegas en otro país. Aunque han acordado no mencionar nombres ni ubicaciones, aún quieren garantizar que sus correos electrónicos y conversaciones a través de mensajería instantánea sobre este tópico se mantengan privadas. Después de convocar a una reunión para ocuparse de la importancia de la seguridad en la comunicación, Claudia pregunta si alguien en la oficina tiene alguna inquietud.

¿Qué puedes aprender de este capítulo?

- Porqué la mayoría de los correos con interfase web y servicios de mensajería instantánea no son seguros.
- Crear una nueva y más segura cuenta de correo electrónico.
- Mejorar la seguridad en tu actual cuenta de correo electrónico.
- Utilizar un servicio seguro de mensajería instantánea.

- Qué hacer en caso que sospeches que alguien podría estar accediendo a tu correo electrónico.
- Verificar la identidad de un corresponsal de correo electrónico.

Asegurar tu correo electrónico

Existen pocos pasos importantes que puedes dar para incrementar la seguridad de tu comunicación por correo electrónico. El primero es asegurarte que sólo la persona a quien le envías el mensaje sea capaz de leerlo. Esto se trata en las secciones **Mantener privado tu correo con interfaz web** y **Cambiarse a una cuenta de correo electrónico más segura**, que vienen a continuación.

Yendo más allá de los fundamentos, a veces es crítico que tus contactos de correo electrónico tengan la capacidad de verificar, sin duda, que un mensaje en particular efectivamente viene de ti y no de alguien que podría estar intentando hacerse pasar por ti. Una manera de lograrlo está en la sección **Seguridad avanzada de correo electrónico**, dentro de la sección **Cifrar y autenticar los mensajes individuales**.

También debes saber que si sospechas que la privacidad de tu cuenta de correo electrónico ha podido ser violada. La sección **Consejos para responder a una sospecha de violación de correo electrónico** se ocupa de esta interrogante.

Recuerda, también, que el asegurar el correo electrónico no tendrá ningún efecto positivo si todo lo que ingresas se registra por medio de un software espía (spyware) y es enviado de manera periódica por medio de la Internet a un tercero. El capítulo **1. Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers)** ofrece algunos consejos sobre como evitar esta clase de cosas, y el capítulo **3. Crear y mantener contraseñas seguras** te ayudará a proteger tus cuentas para el correo electrónico y las herramientas de mensajería instantánea descritas a continuación.

Mantener privado tu correo con interfaz web

La Internet es una red abierta a través de la cual la información normalmente viaja en formato legible. Si un mensaje común de correo electrónico es interceptado en su ruta hacia el destinatario, su contenido puede ser leído muy fácilmente. Y, debido a que la Internet es tan solo una gran red que depende de computadoras intermedias para dirigir el tráfico, muchas personas distintas pueden tener la oportunidad de interceptar un mensaje de esta manera. Tu *Proveedor de Servicio de Internet (ISP)* es el primer destinatario de un mensaje de correo electrónico cuando este inicia su viaje hacia el destinatario final. De manera similar, el ISP del destinatario es la última parada para tu mensaje antes de ser entregado. A menos que tomes ciertas precauciones, tus mensajes pueden ser leídos o interferidos en cualquiera de estos puntos, o en cualquier parte entre ellos.

Pablo: Estuve hablando con uno de nuestros colegas acerca de todo esto, y ella dijo que ella y sus colegas a veces simplemente guardan mensajes importantes en la carpeta de 'Borradores' de su cuenta de correo con interfaz web donde todos comparten una contraseña. Esto me suena un tanto extraño, pero ¿Funciona? Es decir, ¿ese hecho no evitaría que alguien lea los mensajes, ya que en realidad nunca los enviaron?

Claudia: Sea cual fuera el momento en que lees un mensaje de correo electrónico en tu computadora, incluso si es solamente un 'borrador', su contenido ha sido enviado a ti a través de la Internet. De lo contrario, no podría aparecer en tu pantalla ¿correcto? La cosa es que si alguien te tiene bajo vigilancia, ellos simplemente no vigilan tus mensajes de correo electrónico, ellos pueden escanear toda la información legible que sale e ingresa a tu computadora. En otras palabras, este truco no funcionaría al menos que cada uno se conecte de manera segura a esa cuenta compartida con interfaz web. Y si lo hacen entonces no hace daño a nadie crear cuentas separadas o seguir adelante y pulsar el botón de 'enviar'.

Hace tiempo que es posible asegurar tu conexión de Internet entre tu computadora y los sitios web que visitas. A menudo encuentras este nivel de seguridad cuando ingresas contraseñas o información de tarjeta de crédito en sitios web. La tecnología que hace que ello sea posible se llama *cifrado* de *Capa de Conexión Segura (Secure Sockets Layer (SSL))*. Puedes decir si estas o no utilizando SSL mirando con atención la barra de direcciones de tu navegador web.

Todas las direcciones web normalmente empiezan con las letras **HTTP**, como se muestra en el ejemplo siguiente:



Cuando visitas un sito web seguro, su dirección empieza con **HTTPS**.



La ' **S**' adicional al final significa que tu computadora ha establecido una conexión segura al sitio web. También puedes notar un símbolo de 'candado', ya sea en la barra de direcciones o en la barra de estado en la parte baja de tu ventana del navegador. Estas son pistas que te permiten saber que cualquiera que esté vigilando tu conexión a Internet no será ya capaz de espiar tu comunicación con dicho sitio web en particular.

Además de proteger contraseñas e información financiera, este tipo de *cifrado* es perfecto para asegurar tu correo con interfaz web. Sin embargo, muchos proveedores de correos con interfaz web no ofrecen acceso seguro, y otros requieren que lo habilites explícitamente, ya sea fijando una preferencia o ingresando manualmente el termino **HTTPS**. Siempre debes asegurarte que tu conexión sea segura antes de tener acceso, leer tu correo electrónico o enviar un mensaje.

Debes prestar mucha atención si tu navegador de pronto empieza a quejarse sobre unos *certificados de seguridad* inválidos cuando intentas acceder a una cuenta segura con interfaz web. Esto podría significar que alguien esta interfiriendo en la comunicación entre tu computadora y el servidor con el fin de interceptar tus mensajes. Finalmente, si confías en tu correo con interfaz web para intercambiar información sensible, es importante que tu navegador sea lo más confiable posible. Considera el instalar el Mozilla *Firefox* y sus complementos vinculados a la seguridad.

Pablo: Una de las personas que va a trabajar con nosotros en este informe tiende a utilizar su cuenta de correo con interfaz web de Yahoo cuando no está en la oficina. Y si no recuerdo mal alguien más utiliza Hotmail. Si les envío un mensaje a estas personas, ¿Puede otra persona leerlos?

Claudia: Probablemente. Yahoo, Hotmail y otros muchos proveedores de correo con interfaz web tienen sitios web inseguros que no protegen la privacidad de los mensajes de sus usuarios. Vamos a tener que cambiar los hábitos de ciertas personas si deseamos ser capaces de tratar estos testimonios de forma segura.

Cambiarse a una cuenta de correo electrónico más segura

Pocos proveedores de correo con interfaz web ofrecen el acceso *Capa de Conexión Segura (SSL)* a tu correo electrónico. Por ejemplo, Yahoo y Hotmail, proporcionan una conexión segura cuando inicias sesión, para proteger tu contraseña, pero tus mensajes en sí se envían y reciben de manera insegura. Además, Yahoo, Hotmail y otros proveedores de correo con interfaz web incluyen la *dirección IP* de la computadora que estas utilizando en todos los mensajes que envías.

Por otro lado, las cuentas de Gmail, pueden ser utilizadas completamente, a través de una conexión segura, en la medida en la que tu te conectes con tu cuenta desde https://mail.google.com (con la **HTTPS**), en vez de http://mail.google.com. De hecho, puedes ahora fijar una opción que le diga siempre a Gmail que utilice una conexión segura. Y, a diferencia de Yahoo o Hotmail, Gmail evita revelar tu *dirección IP* a los destinatarios de tu correo electrónico. Sin embargo, no se recomienda que confíes ciegamente en Google la confidencialidad de tu comunicación sensible por correo electrónico. Google escanea y registra el contenido de los mensajes de sus usuario para una basta variedad de propósitos y ha, en el pasado, cedido a las demandas de los gobiernos que restringen la libertad digital. Dirígete a la sección de **Lecturas Adicionales** para obtener mayor información sobre la política de privacidad de Google.

Si es posible, debes crearte una nueva cuenta de correo electrónico en *Riseup* visitando https://mail.riseup.net. Riseup ofrece correo electrónico gratuito a los activistas alrededor del mundo y presta mucha atención a la protección de la información almacenada en sus servidores. Ellos por mucho tiempo son una fuente confiable para aquellos con necesidad de soluciones seguras de correo electrónico. Y, a diferencia de Google, tiene políticas muy estrictas relativas a la privacidad de sus usuarios e intereses no comerciales que en algún momento pudieran entrar en conflicto con sus políticas. Sin embargo, con el fin de crear una nueva cuenta de

Riseup, necesitaras dos 'códigos de invitación.' Estos pueden ser entregados por cualquiera que ya tenga una cuenta de Riseup. Si tienes una copia física de este folleto, debes haber recibido tus 'códigos de invitación' junto con el mismo. Si no es así, necesitaras ubicar dos usuarios de Riseup y solicitarles que cada uno de ellos te envíe un código.

Tanto el Gmail como *Riseup* son más que solo proveedores de correo con interfaz web. Estos pueden también utilizarse con un cliente de correo electrónico, tal como el Mozilla *Thunderbird*, que admite las técnicas descritas en **Seguridad avanzada de correo electrónico**. El garantizar que tu cliente de correo electrónico tenga una conexión *cifrada* con tu proveedor es tan importante como el acceder a tu correo con interfaz web a través de una dirección **HTTPS** . Si utilizas un cliente de correo electrónico, dirígete a la **Guía del Thunderbird** para detalles adicionales. Sin embargo, por lo menos, debes estar seguro de habilitar el cifrado *SSL* o **TLS** tanto para los servidores de correo de salida como de entrada.

Pablo: Entonces, ¿debo cambiarme a utilizar el Riseup o puedo seguir utilizando Gmail, y simplemente cambiarme a una dirección 'https'?

Claudia: Esa es tu decisión, pero hay algunas cosas que debes considerar definitivamente cuando elijas un proveedor de correo electrónico. Primero, ¿te ofrecen una conexión segura a tu cuenta? Gmail lo hace, entonces ahí estás bien. Segundo, ¿confías en que los administradores mantengan privado tu correo electrónico y que no lo lean o compartan con otros? Esa depende de ti. Y, finalmente, debes pensar si es o no aceptable para ti que se te identifique con ese proveedor. En otras palabras, te pondrá en problemas el utilizar una dirección de correo electrónico que termine con 'riseup.net', el cual se conoce que es popular entre activistas, o necesitas una dirección más común como 'gmail.com'?

Sin importar que herramientas seguras de correo electrónico decidas utilizar, considera que cada mensaje tiene un remitente y uno o más destinatarios. Tú mismo eres sólo una parte de todo, incluso si accedes a tu cuenta de correo electrónico de manera segura, considera que precauciones toman o no tus contactos cuando envían, leen y responden a los mensajes, trata también de conocer donde se hallan los proveedores de correo electrónico de tus contactos.

Naturalmente, algunos países son más agresivos que otros cuando se trata de vigilancia de correos electrónicos. Para garantizar la comunicación privada, tú y tus contactos deben utilizar servicios de correo electrónico seguros alojados en países relativamente seguros. Y - si quieres estar seguro que tus mensajes no son interceptados entre tu servidor de correo electrónico y el correspondiente de tu contacto - todos deben elegir el utilizar cuentas del mismo proveedor, utilizar el *Riseup* es una buena idea.

Consejos adicionales para mejorar la seguridad de tu correo electrónico

- Siempre se cauto cuando abras archivos adjuntos a un correo electrónico que no estés esperando, que provengan de alguien que no conoces o que contengan términos sospechosos en la línea de asunto. Cuando abras correos electrónicos como estos, debes asegurarte que tu software antivirus esté actualizado y prestar mucha atención a cualquier advertencia que se muestre por parte de tu navegador o tu programa de correo electrónico.
- El utilizar software anónimo como el *Tor*, el cual se describe en el capítulo **8. Mantenerse en el anonimato y evadir la censura en Internet**, puede ayudarte a esconder el servicio de correo electrónico que elegiste de cualquiera que pudiera estar vigilando tu conexión de Internet. Y, dependiendo de la amplitud del filtrado de Internet en tu país, podrías necesitar utilizar Tor, o una de las herramientas de *evasión* descritas en dicho capitulo, sólo para acceder a un proveedor seguro de correo electrónico tal como el *Riseup* o Gmail.
- Cuando crees una cuenta que pretendes utilizar mientras te mantienes anónimo antes tus propios destinatarios de correo electrónico, o de foros públicos en los cuales colocas mensajes por correo electrónico, debes ser lo suficientemente cuidadoso para no registrar un nombre de usuario o 'Nombre Completo' que este relacionado a tu vida personal o profesional. En dichos casos, también es importante que evites utilizar Hotmail, Yahoo, o cualquier otro proveedor de correo con interfaz web que incluya tu

dirección IP en los mensajes que envías.

- Dependiendo de quien tenga acceso físico a tu computadora, el eliminar los rastros vinculados a tu correo electrónico de tus archivos temporales puedes ser tan importante como proteger tus mensajes mientras viajan por la Internet. Dirígete al capítulo **6. Destruir información sensible** y a la **Guía del CCleaner** para obtener detalles.

Consejos para responder ante una sospecha de vigilancia de correo electrónico

Si sospechas que alguien ya está vigilando tu correo electrónico, puedes querer crear una nueva cuenta y conservar la antigua como un señuelo. Sin embargo, recuerda que cualquier cuenta con la cual hayas intercambiado correo electrónico en el pasado podría estar también ahora bajo vigilancia. Como resultado de ello, debes tener algunas precauciones adicionales:

- Tanto tú como tus contactos recientes de correo electrónico deben crear nuevas cuentas y conectarse a ellas sólo desde lugares, como un café Internet, que nunca antes hayan utilizado. Te recomendamos esta estrategia con el fin de evitar conexiones desde la computadora que normalmente usas, la cual puede estar vigilada, y facilitarles a quienes te vigilan la ubicación de tu nueva cuenta. Como alternativa—si vas a iniciar sesión para tu nueva cuenta desde tu ubicación normal—puedes utilizar una de las herramientas descritas en el capítulo **8. Mantenerse en el anonimato y evadir la censura en Internet**, para ocultar estas conexiones.
- Intercambia información sobre esta nueva dirección de correo electrónico solo a través de canales seguros, tales como reuniones cara a cara, mensajes instantáneos seguros o cifrados, conversaciones de *Voz sobre Protocolo de Internet (VoIP)*.
- Mantén casi sin cambios el tráfico en tu vieja cuenta, al menos por un tiempo. Debes aparentar ante el espía que todavía estas utilizando la cuenta para información sensible. Probablemente, desees evitar el revelar información vital, pero debes intentar no hacer obvio que lo estás haciendo. Como puedes imaginar, esto puede ser algo exigente.
- Dificulta el conectar tu identidad real con tu nueva cuenta. No envíes correos electrónicos entre tu nueva cuenta y las antiguas (o las de cualquier contacto del que sospeches que también pueda estar vigilado).
- Mantente atento a lo que escribes cuando utilices tu nueva cuenta. Es mejor que evites utilizar nombres reales y direcciones o frases como 'derechos humanos' o 'tortura.' Desarrolla un sistema de código informal con tus contactos de correo electrónico y cámbialo periódicamente.
- Recuerda. La seguridad del correo electrónico no trata solamente de tener fuertes defensas técnicas. Es también prestar atención a como tú y tus contactos de correo electrónico se comunican y mantienen disciplinados con relación a sus hábitos no técnicos de seguridad.

Asegurar otras herramientas de comunicación por Internet

De manera similar que en el caso del correo electrónico, el software de mensajería instantánea y de *Voz sobre Protocolo de Internet (VoIP)* pueden o no ser seguros, dependiendo de las herramientas que escojas y de como las uses.

Asegurar tu software de mensajería instantánea

La mensajería instantánea, también llamada 'chat,' normalmente no es segura, y puede ser tan vulnerable a la vigilancia como lo es el correo electrónico. Por suerte, existen programas que pueden ayudarte a asegurar la privacidad de tus sesiones de conversación o chat. Sin embargo - del mismo modo que con el correo electrónico - un canal de comunicación seguro requiere que tanto tú como tus contactos de mensajería instantánea utilicen el mismo software y tomen las mismas precauciones de seguridad.

Existe un programa para conversación o chat llamado *Pidgin* que admite muchos de los protocolos existentes de

mensajería instantánea, lo que significa que puedes utilizarlo fácilmente sin tener que cambiar el nombre de tu cuenta o recrear tu lista de contactos. Con el fin de tener conversaciones privadas **cifradas** a través del Pidgin, necesitarás instalar y activar el complemento *Fuera de Registro (OTR)*. Afortunadamente, este es un proceso muy simple.

El *Skype*, que es una herramienta común de *Voz sobre Protocolo de Internet (VoIP)*, también admite la mensajería instantánea. Mientras que el utilizar el Skype es probablemente más seguro que el utilizar una de las alternativas sin el complemento *Fuera de Registro (OTR)*, este tiene dos importantes inconvenientes. Primero, solo te permite conversar (chat) con otros usuarios de Skype, mientras que el *Pidgin* puede utilizarse para comunicarse en forma segura con casi todos los otros servicios de mensajería instantánea. Segundo, debido a que no es de código abierto, es imposible verificar la fortaleza de su **cifrado**. El capitulo **1. Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers)** se ocupa de las virtudes del *Software Libre y de Código Abierto (FOSS)* en su sección **mantener actualizado tu software**. En pocas palabras, es mejor que utilices el Pidgin, con el complemento Fuera de Registro (OTR), para mensajería instantánea segura.

Pablo: Si el correo con interfaz de Yahoo es inseguro, eso significa que el ¿Yahoo Chat es inseguro, también?

Claudia: Lo que tienes que recordar es que, si queremos utilizar mensajería instantánea para ocuparnos de este informe, necesitamos asegurarnos que todas las personas involucradas tengan instalados el Pidgin y el complemento Fuera de Registro (OTR). Si es así, podemos utilizar el Yahoo Chat o cualquier otro servicio de conversación (Chat).

Asegurar tu software de Voz sobre Protocolo de Internet (VoIP)

Las llamadas utilizando *Voz sobre Protocolo de Internet (VoIP)* hacia otros usuarios de Voz sobre Protocolo de Internet (VoIP) son generalmente gratuitas. Algunos programas te permiten también hacer llamadas baratas a teléfonos normales, incluyendo números internacionales. No es necesario decir que estas características pueden ser extremadamente útiles. Algunos de los programas más populares de Voz sobre Protocolo de Internet (VoIP) incluyen al *Skype*, Gizmo [1], Google Talk [2], Yahoo! Voice [3] y el MSN Messenger [4].

Normalmente, la comunicación por voz en Internet no es más segura que el correo electrónico no protegido y la mensajería instantánea. Sólo el *Skype* y Gizmo ofrecen el cifrado para las conversaciones por voz, y sólo si estas llamando a otro usuario de *Voz sobre Protocolo de Internet (VoIP)*, a diferencia de la telefonía móvil o fija. Además, debido a que ninguna de las aplicaciones es de código abierto, expertos independientes han sido incapaces de probarlos completamente y garantizar que son seguros.

Seguridad avanzada de correo electrónico

Las herramientas y conceptos tratados a continuación se recomiendan para usuarios de computadoras experimentados.

Utilizar cifrado de clave pública en correo electrónico

Es posible alcanzar un gran nivel de privacidad con el correo electrónico, incluso con una cuenta de correo electrónico insegura. Para hacer esto, necesitas aprender sobre *cifrado* de clave pública. Esta técnica te permite cifrar mensajes individuales, haciéndolos ilegibles a cualquiera que no sea uno de los destinatarios previstos. El aspecto ingenioso del cifrado de clave pública es que no tiene que intercambiar ninguna información secreta con tus contactos sobre cómo vas a cifrar tus mensajes en el futuro.

Pablo: ¿Pero como funciona todo esto?

Claudia: ¡Puras matemáticas! Cifras tus mensajes hacia un contacto de correo electrónico dado, utilizando su 'clave pública' especial la cual puede distribuir libremente. Luego, ella utiliza su 'clave privada,' la cual

debe guardar cuidadosamente, con el fin de leer dichos mensajes. A su turno, tu contacto utiliza su clave pública para cifrar mensajes que te escribe. De modo que al final, debes intercambiar claves públicas, pero puedes compartirlas abiertamente, sin tener que preocuparte sobre el hecho de que cualquiera que desee tu clave pública pueda obtenerla.

Esta técnica puede utilizarse con cualquier servicio de correo electrónico, incluso con uno que no cuente con un canal de comunicación seguro, debido a que los mensajes individuales son *cifrados* antes de que dejen tu computadora.

Recuerda que al utilizar el *cifrado* puedes atraer la atención hacia ti. El tipo de cifrado utilizado cuando accedes a un sito web seguro, incluyendo una cuenta de correo con interfaz web, se ve a menudo con menor sospecha que la del tipo de cifrado de clave pública del que nos ocupamos aquí. En algunas circunstancias, si un correo electrónico que contenga esta suerte de datos cifrados es interceptado o publicado en un foro público, podría incriminar a la persona que lo envió, sin considerar el contenido del mensaje. Tú a veces tendrías que escoger entre la privacidad de tu mensaje y la necesidad de mantenerte sin llamar la atención.

Cifrar y autenticar mensajes individuales

El *cifrado* de clave pública puede parecer complicado al inicio, pero es muy directo una vez que has entendido los fundamentos, y las herramientas no son difíciles de utilizar. El programa de correo electrónico Mozilla *Thunderbird* puede ser utilizado con un complemento llamado *Enigmail* para cifrar y descifrar muy fácilmente mensajes de correo electrónico.

VauletSuite 2 Go, software gratuito de cifrado de correos electrónicos, es incluso más fácil de utilizar que el Thunderbird si optas por confiar en la compañía que lo provee y permitirle a esta realizar parte del trabajo por ti.

La autenticidad de tu correo electrónico es otro aspecto importante de la seguridad en las comunicaciones. Cualquiera con acceso a la Internet y las herramientas correctas puede suplantarte enviando mensajes desde un correo electrónico falso que sea idéntico al tuyo. El peligro aquí es más aparente cuando se considera desde la perspectiva del destinatario. Imagina, por ejemplo, la amenaza planteada por un correo electrónico que aparenta ser de un contacto confiable pero que es en realidad de alguien cuyo objetivo es el de perturbar tus actividades o conocer información sensible sobre tu organización.

Debido a que no podemos ver o escuchar a nuestros corresponsales a través del correo electrónico, normalmente confiamos en la dirección del remitente para verificar su identidad, que es la razón por la cual somos fácilmente engañados por correos electrónicos falsos. Las *firmas digitales* - las cuales también se sostienen en *cifrado* de clave pública - proporcionan un medio más seguro de probar la identidad de uno cuando se envía un mensaje. La sección de **Utilizar Enigmail con Thunderbird** de la **Guía del Thunderbird** explica en detalle como se hace esto.

Pablo: Tengo un colega que una vez recibió un correo electrónico de parte mía que nunca envié. Decidimos, al final, que simplemente era correo comercial no deseado (spam), pero ahora me imagino cuanto daño podría haberse hecho si un correo electrónico falso apareciera en el buzón de la persona equivocada en el momento inapropiado. Escuche que se puede impedir esta clase de evento con firmas digitales ¿pero que son ellas?

Claudia: Una firma digital es como un sello lacrado sobre la solapa de un sobre con tu carta incluida. Excepto que no puede falsificarse. Esto prueba que eres el verdadero remitente del mensaje y que este no ha sido falsificado en el camino.

8. Mantenerse en el anonimato y evadir la censura en Internet

Muchos países alrededor del mundo han instalado software que evita que los usuarios dentro de ese país puedan acceder a ciertos sitios web y servicios de Internet. Las compañías, colegios y bibliotecas públicas a menudo utilizan un software similar para proteger a sus empleados, estudiantes y clientes de material que consideran molesto o dañino. Este tipo de tecnología de filtrado viene en diferentes formas. Algunos filtros bloquean sitios de acuerdo a su *dirección IP*, mientras otros ponen en su lista negra ciertos *nombres de dominio* o buscan a través de todas las comunicaciones no cifradas en Internet palabras claves específicas.

Sin importar que métodos de filtrado se hallen presentes, casi siempre es posible evadirlos confiando en computadoras intermediarias, fuera del país, para acceder a servicios bloqueados para ti. Este proceso a menudo se llama *evasión* de la censura, o simplemente evasión, y las computadoras intermedias se llaman *proxies*. También existen proxies de diferentes formas. Este capitulo incluye un breve tratamiento de redes de anonimato multiproxy seguido de una descripción más al detalle de proxies de evasión básica y de cual es su forma de funcionamiento.

Ambos métodos son maneras efectivas de evadir los filtros de Internet, aunque el primero es más apropiado si estas dispuesto a sacrificar velocidad con el fin de mantener tus actividades en Internet lo más anónimas posibles. Si conoces y confías en la persona o en la organización que opera tu *proxy*, o si el desempeño es más importante para ti que el anonimato, entonces un proxy de *evasión* básica te será más útil.

Contexto

Mansour y Magda son hermanos, en un país de habla árabe, que mantienen una bitácora (blog) en la cual anónimamente hacen público los abusos de derechos humanos y hacen campaña por un cambio político. Las autoridades en su país no han sido capaces de cerrar su sito web, debido a que está alojado en otro país, pero a menudo han intentado conocer la identidad de los administradores de la bitácora (blog) a través de otros activistas. A Mansour y Magda les preocupa que las autoridades sean capaces de vigilar sus actualizaciones y saber quienes son. Además, desean prepararse para cuando finalmente el gobierno filtre su sitio web, para no sólo continuar actualizándolo, sino también que puedan proporcionar un buen consejo de evasión para sus lectores dentro de su propio país, quienes de otro modo perderían acceso a la bitácora (blog).

¿Qué puedes aprender de esta capítulo?

- Acceder a un sitio web que esté bloqueado dentro de tu país
- Evitar que los sitios web que visitas sepan tu ubicación
- Garantizar que ni tu *Proveedor de Servicios de Internet (ISP)* ni una organización de vigilancia en tu país puedan determinar que sitios web o servicios de Internet visitas

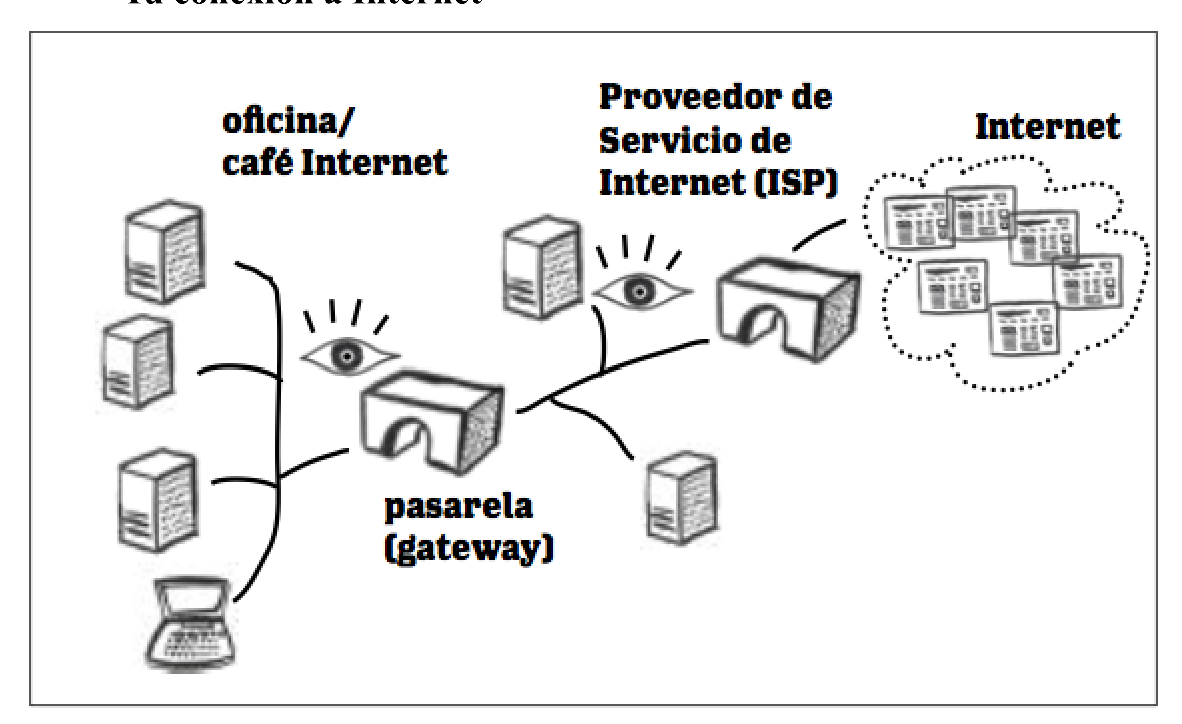
Comprender la censura en Internet

Las investigaciones llevadas a cabo por organizaciones como OpenNet Initiative (ONI) [1] y Reporteros Sin Fronteras (RSF) [2] indican que muchos países filtran una amplia variedad de contenido social, político y de 'seguridad nacional', aunque raramente publican listas precisas de lo que ha sido bloqueado. Naturalmente, aquellos que desean controlar el acceso de sus ciudadanos a la Internet también hacen un esfuerzo especial para bloquear *proxies* y sitios web conocidos que ofrecen herramientas e instrucciones para ayudar a las personas a evadir estos filtros.

A pesar de la garantía de libre acceso a la información consagrada en el Artículo 19 de la Declaración Universal de los Derechos Humanos, el número de países involucrados en la censura de Internet se ha incrementado espectacularmente en los últimos años. Sin embargo, a medida que la práctica de filtrado de Internet se disemina en el mundo, de igual manera lo hace el acceso a las herramientas de evasión que han sido creadas, utilizadas y publicitadas por activistas, programadores y voluntarios.

Antes de explorar las distintas maneras de evadir la censura en Internet, primero debes desarrollar un entendimiento básico de cómo funcionan estos filtros. Para hacerlo, es muy útil considerar un modelo altamente simplificado de tu conexión a Internet.

Tu conexión a Internet



El primer paso de tu conexión a la Internet se hace típicamente a través del *Proveedor de Servicio de Internet (ISP)* en casa, oficina, colegio, biblioteca o café Internet. El Proveedor de Servicio de Internet (ISP) le asigna a tu computadora una *dirección IP*, la cual puede ser utilizada por varios servicios de Internet para identificarte y enviarte información, tales como los correos electrónicos y páginas web que solicites. Cualquiera que conozca tu dirección IP puede saber más o menos en que ciudad te hallas. Sin embargo, algunas organizaciones bien conectadas en tu país, pueden utilizar esta información para determinar tu ubicación precisa.

- **Tu Proveedor de Servicio de Internet (ISP)** sabrá en que edificio estás o que línea telefónica estás utilizando si accedes a Internet a través de un módem.
- **Tu café Internet, biblioteca o negocio** sabrá que computadora estuviste utilizando en un momento determinado, así como a que puerto o a que punto de acceso inalámbrico estuviste conectado.
- **Las agencias gubernamentales** pueden conocer todos estos detalles, como resultado de su influencia sobre las organizaciones arriba mencionadas.

En este punto, tu *Proveedor de Servicio de Internet (ISP)* descansa en la infraestructura de la red en tu país para conectar a sus usuarios, incluyéndote, con el resto del mundo. En el otro extremo de tu conexión, el sitio web o el servicio de Internet al cual estás accediendo pasa a través de un proceso similar, habiendo recibido su propia dirección IP de su Proveedor de Servicio de Internet (ISP) en su propio país. Incluso sin todos los detalles técnicos, un modelo básico como este puede ser útil cuando piensas en las varias herramientas que te permiten rodear los filtros y mantenerte anónimo en la Internet.

Cómo son bloqueados los sitios web

Esencialmente, cuando vas a visualizar una página web, le estás mostrando la *dirección IP* del sitio a tu *Proveedor de Servicio de Internet (ISP)* y solicitándole conectarte con el Proveedor de Servicio de Internet (ISP) del servidor web. Y - si tienes una conexión de Internet no filtrada - hará justamente eso. Sin embargo, si te encuentras en un país que censura la Internet, este consultará primero la *lista negra* de sitios web prohibidos y luego decidirá si accede o no a tu solicitud.

En algunos casos, puede haber una organización central que maneja el filtrado en lugar de los mismos *Proveedor de Servicio de Internet (ISP)*. A menudo, una *lista negra* contendrá *nombres de dominio*, tales como www.blogger.com, en vez de *direcciones IP*. Y, en algunos países, el software de filtrado controla tu conexión, en vez de intentar bloquear direcciones específicas en Internet. Este tipo de software escanea las solicitudes que hiciste y las páginas que regresan a ti, buscando palabras claves sensibles para luego decidir si te permite o no ver los resultados.

Y, para empeorar las cosas, cuando una página web es bloqueada no podrías ni siquiera saberlo. Aunque algunos filtros proporcionan una 'página de bloqueo' que explica porque una página en particular ha sido

censurada, otras muestran mensajes de error desorientadores. Estos mensajes pueden implicar que la página no puede ser encontrada, por ejemplo, o que la dirección fue mal ingresada.

En general, lo más fácil es adoptar la perspectiva correspondiente al peor caso hacia la censura de Internet, en vez de intentar investigar todas las fortalezas y debilidades de las tecnologías de filtrado utilizadas en tu país. En otras palabras, puedes asumir que:

- Tu tráfico en Internet está controlado por palabras claves.
- El filtrado está implementado directamente al nivel del *Proveedor de Servicio de Internet (ISP)*.
- Los sitios bloqueados son considerados en *listas negras* tanto por las *direcciones IP* como por *nombres de dominio*.
- Se te pueden dar razones oscuras o desorientadoras para explicar porque un sitio bloqueado no se descarga.

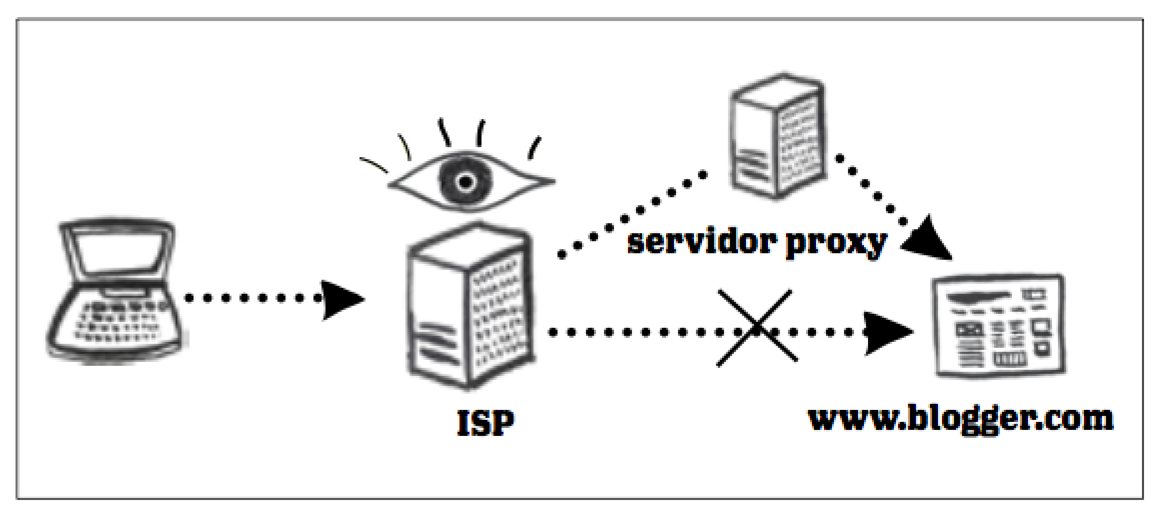
Debido a que las herramientas de evasión más efectivas pueden ser utilizadas sin importar que métodos de filtrado están en funcionamiento, generalmente no hace daño hacer esta asunción pesimista.

Mansour: Entonces, si un día me encuentro con que no puedo acceder a la bitácora (blog), pero un amigo en otro país puede verlo sin problemas, ¿eso significa que el gobierno lo ha bloqueado?

Magda: No necesariamente. Podría ser algún problema que sólo afecta a las personas que están tratando de acceder al sitio web desde aquí. O, podría ser algún problema con tu computadora que sólo se muestra con ciertos tipos de páginas web. Sin embargo estás en la ruta correcta. Podrías también intentar visitarla mientras utilizas una herramienta de evasión. Después de todo, la mayoría de estas herramientas descansan en servidores proxy externos, cuyo funcionamiento se parece al hecho de pedirle a un amigo en otro país que pruebe un sitio web para ti, excepto que puedes hacerlo por ti mismo

Entender la evasión de la censura

Si no puedes acceder directamente a un sitio web debido a que está bloqueado por uno de los métodos tratados anteriormente, necesitas encontrar una forma de rodear la obstrucción. Un servidor *proxy* seguro, localizado en un país que no filtra la Internet puede proporcionar esta clase de desvío buscando las páginas web que solicitas y enviándotelas. Desde la perspectiva de tu *Proveedor de Servicio de Internet (ISP)* aparecerás simplemente comunicándote de manera segura con una computadora desconocida (el servidor proxy) en algún lugar de la Internet.



Obviamente, la agencia gubernamental a cargo de la censura de Internet en tu país—o la compañía que proporciona actualizaciones para su software de filtrado—podría finalmente saber que esta 'computadora desconocida' es realmente un *proxy* de evasión. Si esto ocurre, su *dirección IP* puede ser añadida a la *lista negra*, y no funcionará más. Sin embargo, normalmente toma algún tiempo el bloqueado de los proxies, y aquellos quienes crean y actualizan las herramientas de evasión son concientes de esta amenaza. Ellos responden utilizando uno o los dos métodos mostrados a continuación:

- Los **Proxies escondidos** son más difíciles de identificar. Esta es una de las razones por la que es

importante utilizar *proxies* seguros, los cuales son menos obvios. Sin embargo, el *cifrado* es sólo parte de la solución. Los operadores de un proxy también deben ser cuidadosos cuando dan su ubicación a nuevos usuarios si desean que este se mantenga escondido.

- Los **Proxies desechables** pueden ser reemplazados muy rápidamente después de ser bloqueados. El proceso de informar a los usuarios como hallar los *proxies* de reemplazo puede no ser particularmente seguro. En vez de ello, las herramientas de evasión de este tipo a menudo simplemente tratan de distribuir nuevos proxies más rápido que su proceso de bloqueo.

Al final, mientras sea posible tener a la mano un *proxy* confiable para que te traiga los servicios que solicitas, todo lo que debes hacer es enviar tu solicitud y ver que regrese utilizando la aplicación apropiada de Internet. Normalmente, los detalles de este proceso son manejados automáticamente por el software de evasión que instalaste en tu computadora, al modificar las opciones de tu navegador o dirigiendolo a una página proxy basada en la web. La red anónima *Tor*, descrita en las sección siguiente, utiliza el primer método. A continuación viene el tópico de herramientas de evasión proxy básicas, únicas, cada una de las cuales funciona de manera ligeramente diferente.

Redes anónimas y servidores proxy básicos

Redes anónimas

Las redes anónimas normalmente 'hacen rebotar' tu tráfico de Internet entre varios *proxies* seguros con el fin de disfrazar de donde vienes y a que estas tratando de acceder. Esto puede reducir significativamente la velocidad a la cual eres capaz de descargar las páginas web y otros servicios de Internet. Sin embargo, en el caso de *Tor*, este también te proporciona un medio confiable, seguro y público de evasión que te ahorra el preocuparte si confías o no en las personas que operan tus proxies y los sitios web que visitas. Como siempre, debes garantizar que tienes una conexión cifrada, utilizando *HTTPS*, para un sitio web seguro antes de intercambiar información sensible, tal como contraseñas y correos electrónicos, a través de un navegador.

Tienes que instalar software para utilizar el *Tor*, pero el resultado es una herramienta que te proporciona anonimato así como evasión. Cada vez que te conectas a la red del Tor, seleccionas una ruta aleatoria a través de tres proxies seguros del Tor. Esto garantiza que ni tu *Proveedor de Servicio de Internet (ISP)* ni los mismos proxies conozcan la *dirección IP* de tu computadora ni la ubicación de los servicios de Internet que solicitas. Puedes aprender más sobre esta herramienta en la Guía del Tor.

Una de las fortalezas del *Tor* es que no solo trabaja con navegador sino que puede ser utilizado con varios tipos de software de Internet. Los programas de correo electrónico, entre ellos el Mozilla *Thunderbird*, y los programas de mensajería instantánea, incluyendo al *Pidgin*, pueden ser operados a través del Tor, ya sea para acceder a servicios filtrados o para esconder el uso que le das a dichos servicios.

Proxies básicos de evasión

Existen tres importantes características que debes considerar cuando seleccionas un *proxy* básico de evasión. Primero, ¿es una herramienta basada en la web? o ¿requiere que cambies las opciones o que instales software en tu computadora? Segundo, ¿es seguro? Tercero, ¿es público o privado?

Proxies basados en la web y otros:

Los *proxies* basados en la web son probablemente los más fáciles de usar. Ellos sólo requieren que apuntes tu navegador hacia una página web proxy, ingreses la dirección filtrada que deseas ver y pulses un botón. El proxy entonces mostrará el contenido solicitado dentro de su propia página web. Puedes normalmente seguir los enlaces o ingresar una nueva dirección en el proxy si deseas ver una nueva página. No necesitas instalar ningún software o cambiar alguna opción de navegador, lo cual significa que los proxies basados en la web son:

- Fáciles de usar
- Asequibles desde computadoras públicas, como aquellas en los cafés Internet, las cuales no podrían permitirte instalar programas o cambiar opciones
- Son potencialmente seguros si estás preocupado acerca de ser 'sorprendido' con software de evasión en

tu computadora.

Los *proxies* basados en la web también tienden a tener ciertas desventajas. No siempre muestran correctamente las páginas, y muchos proxies basados en la web no lograrán descargar sitios web complejos, entre ellos los que presentan archivos de audio simultáneo y contenido de video. Además, mientras que un proxy se hará mas lento mientras sea utilizado por más usuarios, esto podría ser más problemático con los proxies públicos basados en la web. Y, obviamente, los proxies basados en la web sólo funcionan para páginas web. No puedes, por ejemplo, utilizar un programa de mensajería instantánea o un cliente de correo electrónico para acceder a servicios bloqueados a través de un proxy basado en la web. Finalmente, los proxies seguros basados en la web ofrecen una confidencialidad limitada debido a que ellos mismos deben acceder y modificar la información de retorno hacia ti proveniente de los sitios web que visitas. Si no lo hicieran, serías incapaz de pulsar en un enlace sin dejar atrasado al proxy e intentar hacer una conexión directa hacia la página web objetivo. Esto se trata más adelante en la sección siguiente.

Otros tipos de *proxies* generalmente requieren que instales un programa o configures una dirección externa de un proxy en tu navegador o sistema operativo. En el primer caso, tu programa de evasión normalmente proporcionará alguna forma de activar y desactivar la herramienta, para indicarle a tu navegador si debe o no utilizar el proxy. El software de este tipo a menudo te permite cambiar automáticamente de proxies si uno de ellos es bloqueado, como se trató anteriormente. En el segundo caso, necesitarás saber la dirección correcta del proxy, la cual cambiará si dicho proxy es bloqueado o se vuelve tan lento que se convierta en inútil.

Aunque esto puede ser ligeramente más difícil de utilizar que un *proxy* basado en la web, este método de evasión esta mejor dotado para mostrar páginas complejas de manera correcta y le tomará mucho más tiempo ralentizarse a medida que las personas utilicen un proxy dado. Además, pueden encontrarse proxies para varias aplicaciones diferentes de Internet. Los ejemplos incluyen proxies HTTP para navegadores, SOCKS para programas de correo electrónico y mensajería (chat) y VPN que pueden redireccionar todo tu tráfico de Internet para evitar el filtrado.

Proxies seguros e inseguros:

Un *proxy* seguro, en este capitulo, se refiere a cualquier proxy que permita conexiones *cifradas* de sus usuarios. Un proxy inseguro te permitirá evadir muchos tipos de filtro pero fracasará si tu conexión de Internet esta siendo escaneada en busca de palabras claves o de direcciones de páginas web. Es especialmente malo utilizar un proxy inseguro para acceder a sitios web que normalmente están cifrados, tales como aquellos de cuentas de correo electrónico con interfaz web y páginas web bancarias. Al hacerlo, podrías estar exponiendo información sensible que normalmente estaría escondida. Y, como se mencionó anteriormente, los proxies inseguros a menudo son más fáciles de descubrir y bloquear por parte de aquellos que actualizan el software y la políticas de filtrado de Internet. Al final, el hecho de que existan proxies libres, rápidos, seguros significa que existen muy pocas razones para decidirse por uno inseguro.

Tu sabrás si un *proxy* basado en la web es seguro o inseguro si puedes acceder a las mismas páginas web del proxy utilizando direcciones *HTTPS*. Del mismo modo que con los servicios de correo con interfaz web, las conexiones seguras e inseguras pueden ser admitidas, de modo que debes estar seguro de utilizar una dirección segura. A menudo, en dichos casos, deberás aceptar una 'advertencia de certificado de seguridad' de tu navegador con el fin de continuar. Este es el caso para los proxies *Psiphon* y *Peacefire*, que se tratan a continuación. Advertencias como estas te indican que alguien, como tu *Proveedor de Servicio de Internet (ISP)* o un *pirata informático (hacker)*, podría estar vigilando tu conexión al proxy. A pesar de estas advertencias, es una buena idea utilizar proxies seguros en la medida de lo posible. Sin embargo, cuando confíes en tales proxies para evasión, debes evitar visitar sitios web seguros, ingresar contraseñas o intercambiar información sensible a menos que verifiques la huella digital *Capa de Conexión Segura (SSL)* del proxy. Con el fin de hacer esto, necesitarás una manera de comunicarte con el administrador del proxy.

El Apéndice C de la Guía de Usuario del Psiphon [3] explica los pasos que tanto tú, como el administrador del *proxy* deben dar para verificar la huella digital del proxy.

También debes evitar acceder a información sensible a través de un *proxy* basado en la web a menos que confíes en la persona que lo dirige. Esto se aplica sin importar si ves o no una advertencia de certificado de seguridad cuando visitas el proxy. Incluso se aplica si conoces lo suficiente al operador del proxy para verificar la huella digital del servidor antes de dirigir tu navegador a aceptar la advertencia. Cuando confías en un único proxy para la evasión, su administrador conocerá en todo momento tu *dirección IP* y el sitio web al que estás

accediendo. Sin embargo, es mucho más importante considerar que si ese proxy está basado en la web, un operador malicioso podría tener acceso a toda la información que pasa entre tu navegador y los sitios web que visitas, incluyendo el contenido de tu correo con interfaz web y tus contraseñas.

Para los *proxies* que no están basados en la web, debes investigar un poco para determinar si admiten conexiones seguras o inseguras. Todas los proxies y las redes anónimas recomendadas en este capitulo son seguros.

Proxies privados y públicos:

Los *proxies* públicos aceptan conexiones de cualquiera, mientras que los privados normalmente requieren un nombre de usuario y una contraseña. Mientras que los proxies públicos tienen la obvia ventaja de estar disponibles libremente, asumiendo que puedan ser hallados, estos tienden a saturarse muy rápidamente. Como resultado de ello, aunque los proxies públicos sean técnicamente tan sofisticados y bien mantenidos como los privados, estos son a menudo relativamente lentos. Finalmente, los proxies privados tienden a ser dirigidos ya sea por lucro o por administradores que crean cuentas para sus usuarios a quienes conocen personal o socialmente. Debido a esto, es generalmente muy fácil determinar que motiva a un operador de un proxy privado. Sin embargo, no debes asumir que los proxies privados son por tanto básicamente más confiables. Después de todo, motivos de lucro han conducido en el pasado a los servicios en línea a exponer a sus usuarios.

Proxies simples, inseguros y públicos pueden a menudo encontrarse ingresando términos como 'proxy público' en un buscador, pero no debes confiar en proxies descubiertos de esta manera. Dada la oportunidad, es mejor utilizar un proxy seguro y privado conducido por personas que conoces y en las que confías, ya sea personalmente o por su reputación, y quienes tienen las habilidades técnicas para mantener su servidor seguro. Ya sea que utilices o no un proxy basado en la web dependerá de tus particulares necesidades y preferencias. En cualquier momento en que utilices un proxy para evasión, es una buena idea utilizar también el navegador *Firefox* e instalar el complemento *NoScript*, como se trató en la **Guía del Firefox**. El hacerlo puede ayudarte a protegerte tanto de proxies maliciosos como de sitios web que pueden tratar de descubrir tu verdadera *dirección IP*. Finalmente, ten en cuenta que incluso un proxy *cifrado* no tornará un sitio web inseguro en uno seguro. Debes garantizar que tienes una conexión *HTTPS* antes de enviar o recibir información sensible.

Si eres incapaz de encontrar en tu país una persona, una organización o una compañía cuyo servicio *proxy* consideres confiable, asequible y accesible, debes pensar en utilizar la red anónima del *Tor*, de la cual nos ocupamos anteriormente en la parte de **Redes anónimas**.

Proxies específicos de evasión.

A continuación hay unas cuantas herramientas y *proxies* específicos que pueden ayudarte a evadir el filtrado de Internet. Nuevas herramientas de evasión son producidas regularmente, y las existentes son actualizadas frecuentemente, por tanto para saber más debes visitar el sitio web en línea de la **Caja de Herramientas de Seguridad**, y los sitios mencionados en las sección de **Lecturas Adicionales** que se halla a continuación.

Psiphon2 es un sistema de servidores proxy web privado y anónimo. Parta utilizar psiphon2 [4] necesitas la dirección web (URL) del servidor proxy y una cuenta (nombre de usuario y contraseña). Puedes recibir una invitación para crear una cuenta en el psiphon2 de un usuario que ya tenga una cuenta de este tipo. También puedes utilizar la invitación incluida en la versión impresa del folleto guía. Por favor, dirígete a la Guía de Usuario del Psiphon [3].

Sesawe Hotspot Shield, es un proxy de evasión público, seguro, no basado en la web y gratuito. Para utilizarlo, necesitas descargar la herramienta [5] e instalarla. La compañía que desarrolla el Hotspot Shield recibe fondos de anunciantes, de modo que veras una 'pancarta publicitaria' en la parte superior de la ventana de tu navegador cada vez que lo uses para visitar sitios web que no proporcionan *cifrado*. A pesar de que es imposible de verificar, esta compañía afirma borrar la *dirección IP* de quienes utilizan la herramienta, en vez de almacenarla o enviarla a sus anunciantes. Debido a que Hotspot Shield confía en una Red Virtual Privada (RVP), toda tu conexión a Internet pasará a través de un proxy mientras estés 'conectado'. Ello podría ser útil si utilizas proveedores de correo electrónico o mensajería instantánea que son filtrados en tu país. Puedes aprender más del Hotspot Shield en la página web de AnchorFree [6].

Your-Freedom es un *proxy* de evasión privado, seguro y no basado en la web. Esta es una herramienta de

software gratuito (freeware) que puede utilizarse para acceder a un servicio de evasión sin costo. También puedes pagar un cargo para acceder a un servicio comercial, el cual es más rápido y tiene mucho menos limitaciones. Con el fin de utilizar *Your-Freedom*, necesitarás descargar la herramienta [7] y crear una cuenta [8], ambas acciones pueden realizarse en el sitio web de Your-Freedom [9]. De manera similar necesitarás configurar tu navegador para utilizar el proxy cuando te conectes a la Internet. Puedes aprender a hacer esto en el sitio web del Proyecto Sesawe [10].

El **Peacefire** mantiene un gran número de *proxies* públicos basados en la web, los cuales pueden ser seguros e inseguros dependiendo de como accedes a ellos. Cuando utilices el proxy *Peacefire*, debes ingresar la dirección *HTTPS* con el fin de tener una conexión segura entre tú y el proxy. Los nuevos proxies se anuncian a través de una larga lista de correo de manera regular. Pueden inscribirte para recibir actualizaciones en el sito web de Peacefire [11].

Mansour: ¡Excelente! De modo que nuestro Proveedor de Servicio de Internet (ISP) no puede ver lo que estamos hacienda cuando utilizo un servidor proxy, ¿correcto?

Magda: En tanto que utilicemos un proxy seguro, y le demos unos minutos a cada 'advertencia de certificado de seguridad' que pueda aparecer, entonces si, es verdad. Ten en cuenta que los proxies inseguros te permitirán evadir la mayoría de los filtros de Internet, pero también le permitirán a tu Proveedor de Servicio de Internet (ISP) fisgonear en tu conexión, incluyendo la localización de las páginas que estas visitando.

Glosario

Algunos de los términos técnicos que encontrarás, a medida que leas estos capítulos, se define a continuación:

- **Amenaza física** – En este contexto, cualquier amenaza a tu información sensible que sea el resultado de la acción de otras personas que tengan acceso físico directo al hardware de tu computadora o cuyo origen sea otro riesgo físico tal como una rotura, accidente o desastre natural.
- **Archivo de paginación o intercambio** – Archivo en tu computadora en el cual se guarda información, parte de la cual puede ser sensible, ocasionalmente con el fin de mejorar su rendimiento.
- **Arrancado** – Acción de iniciar una computadora.
- **Avast** – Herramienta antivirus de software gratuito.
- **Base de datos de contraseñas seguras** – Herramienta que puede cifrar y almacenar tus contraseñas utilizando una única contraseña maestra.
- **Cable de seguridad** – Cable de cierre que puede utilizarse para asegurar, a una pared o un escritorio, una computadora portátil u otros equipos, entre ellos discos duros externos y algunas computadoras de escritorio. Ello con el fin de impedir que sean físicamente removidos del lugar.
- **Capa de Conexión Segura (Secure Sockets Layer (SSL))** – Tecnología que te permite mantener una conexión segura, *cifrada* entre tu computadora y algunos de los sitios web y los servicios de Internet que visitas. Cuando estas conectado a un sitio web a través de una capa de conexión segura (SSL), la dirección del sitio web empezará con *HTTPS* en vez de *HTTP*.
- **CCleaner** – Herramienta de software libre que elimina los archivos temporales y los potencialmente sensibles rastros dejados en tu disco duro por programas que utilizaste recientemente y por el mismo sistema operativo Windows.
- **Certificado de seguridad** – Forma de garantizar que los sitios web y otros servicios de Internet, utilizando cifrado, son realmente quienes dicen ser. Sin embargo, con el fin de que tu navegador acepte un *certificado de seguridad* como valido, el servicio debe pagar por una *firma digital* de una organización confiable. Debido a que ello es oneroso algunos operadores de servicios son reticentes o incapaces de gastar en este. Sin embargo, de manera ocasional verás un error de *certificado de seguridad* incluso cuando visitas un servicio válido.
- **Cifrado** – Forma ingeniosa de utilizar las matemáticas para *cifrar*, o mezclar, información de modo que

solo pueda ser *descifrada* y leída por quien tenga cierta información, tal como una contraseña o una *llave de cifrado*.

- **Clam Win** – Programa antivirus de software libre y de código abierto para Windows.
- **Cobian Backup** – Herramienta de respaldo de software libre y de código abierto. La última versión del Cobian es de software gratuito pero de código cerrado, sin embargo, las versiones anteriores fueron lanzadas como software gratuito y de código abierto.
- **Código fuente** – Código subyacente escrito por los programadores de computadoras que permite la creación de software. El código fuente para una herramienta dada revelará como funciona y si esta puede ser insegura o maliciosa.
- **Código mnemotécnico** – Un sistema simple que puede ayudarte a recordar contraseñas complejas.
- **Comodo Firewall** – Herramienta cortafuegos de software libre.
- **Cookie** – Pequeño archivo, que almacena tu navegador en tu computadora. Este puede utilizarse para almacenar información de, o para identificarte, en un sitio web particular.
- **Corriente Eléctrica Ininterrumpida (UPS)** – Equipo que permite a tus equipos de computación críticos que continúen operando, o que se apaguen paulatinamente ante la ocurrencia de una breve pérdida de energía.
- **Cortafuegos (firewall)** – Herramienta que protege a tu computadora de conexiones no confiables desde o hacia redes locales y la Internet.
- **Dirección de Protocolo de Internet (dirección IP)** – Identificador único asignado a tu computadora cuando se conecta a Internet.
- **Eliminación Permanente** – Proceso de borrado de información de manera segura y permanente.
- **Enigmail** – Complemento del programa de correo electrónico Thunderbird que le permite a este enviar y recibir correos electrónicos cifrados y firmados digitalmente.
- **Enrutador (router)** – Equipo de red a través del cual las computadoras se conectan a sus redes locales y por medio del cual varias redes locales acceden a Internet. *Interruptores (switches), pasarelas (gateways) y concentradores (hubs)* realizan tareas similares, del mismo modo que los puntos de acceso inalámbricos para computadoras que están apropiadamente equipadas para utilizarlos.
- **Eraser** – Herramienta que elimina información, de tu computadora o de tu dispositivo removible de almacenamiento, de manera segura y permanente.
- **Esteganografía** – Cualquier método de disfrazar información sensible de modo que aparezca ser algo distinto. Ello se hace con el fin de evitar atraer la atención hacia esta.
- **Evasión** – Acto de evadir los filtros de Internet para acceder a los sitios web y otros servicios de Internet bloqueados.
- **Firefox** – Popular navegador web de software libre y de código abierto que es una alternativa al Internet Explorer de Microsoft.
- **Firma Digital** – Forma de utilizar el cifrado para probar que un archivo o mensaje particular fue realmente enviado por la persona que afirma haberlo enviado.
- **Fuera de Registro (OTR)** – Complemento de cifrado del programa de mensajería instantánea *Pidgin*.
- **GNU/Linux** – Sistema operativo de software libre y código abierto que es una alternativa a Windows de Microsoft.
- **HTTPS** – Cuando estas conectado a un sitio web a través de una Capa de Conexión Segura (Secure Socket Layer (SSL)), la dirección del sitio web empezará con HTTPS en vez de HTTP.
- **KeePass** – Software libre de base de datos de contraseñas seguras
- **Lista negra** – Lista de sitios web y otros servicios de Internet bloqueados que no puede ser accedidos debido a una política restrictiva de filtrado.

- **Lista blanca** – Lista de sitios web o de servicios de Internet a los cuales cierta forma de acceso esta permitido, mientras que otros sitios son automáticamente bloqueados.
- **LiveCD** - Un CD que permite a tu computadora ejecutar un sistema operativo diferente en forma temporal.
- **Nombre de dominio** – La dirección, en palabras, de un sitio web o de un servicio de Internet; por ejemplo: security.ngoinabox.org
- **NoScript** – Complemento de seguridad para el navegador Firefox que te protege de programas maliciosos que podrían presentarse en páginas web desconocidas.
- **Peacefire** – Los suscriptores a este servicio gratuito reciben correos electrónicos periódicos que contienen una lista actualizada de proxies de evasión, los cuales pueden ser utilizados para eludir la censura en Internet.
- **Pidgin** – Herramienta de mensajería instantánea de software libre y de código abierto que se apoya en un complemento llamado *Fuera de Registro (OTR)*.
- **Pirata informático (hacker)** – En este contexto, un criminal informático malicioso quien puede intentar acceder a tu información sensible o tomar control de tu computadora de manera remota.
- **Política de seguridad** – Documento escrito que describe cómo tu organización puede protegerse de mejor manera de distintas amenazas, esta incluye una lista de pasos a seguir en caso ocurran ciertos eventos vinculados a la seguridad.
- **Proveedor de Servicio de Internet (ISP)** – La compañía u organización que provee tu conexión inicial a la Internet. Los gobiernos de muchos países ejercen control sobre la Internet, utilizando medios tales como el filtrado y la vigilancia, a través de los proveedores de servicios de Internet que operan en dichos países.
- **Proxy** – Servicio intermediario a través del cual puedes conducir algunas o todas tus comunicaciones por Internet y que puede ser utilizado para evadir la censura en Internet. Un proxy puede ser público, o podrías necesitar un nombre de usuario y una contraseña para conectarte a este. Solamente algunos proxies son seguros, lo que significa que utilizan cifrado para proteger la privacidad de la información que pasa entre tu computadora y los servicios de Internet a los cuales te conectas a través del proxy.
- **Quemador de CD** – Unidad CD-ROM de una computadora que puede escribir datos en CDs en blanco. Los *Quemadores de DVD* pueden hacer lo mismo con DVDs in blanco. Las *unidades de CD-RW* y *de DVD-RW* pueden borrar y reescribir información más de una vez en el mismo CD o DVD que cuente con estas características.
- **Registrador de teclas (keylogger)** – Tipo de software espía que registra que teclas has pulsado en el teclado de tu computadora y envía esta información a un tercero. Los registradores de teclas (keyloggers) son utilizados frecuentemente para robar correos electrónicos y otras contraseñas.
- **Riseup** – Servicio de correo electrónico administrado por y para activistas. A este servicio se puede acceder de manera segura a través de un servidor web de correo o utilizando un cliente de correo electrónico como el *Mozilla Thunderbird*.
- **Servidor** – Computadora que se mantiene encendida y conectada a la Internet con el fin de proporcionar algún servicio, como puede ser el alojamiento de una página web o el envío y recepción de correo electrónico a otras computadoras.
- **Sistema Básico de Entrada/Salida (BIOS)** – El primer y más profundo nivel de software en una computadora. El BIOS te permite fijar muchas opciones avanzadas vinculadas al hardware de la computadora, entre ellas la contraseña de encendido.
- **Skype** – Herramienta de software libre de voz sobre protocolo de Internet (VoIP) que te permite hablar gratuitamente con otros usuarios de Skype y hacer llamadas telefónicas pagando una tarifa. La compañía que respalda el Skype afirma que las conversaciones con otros usuarios de Skype son cifradas. Debido a que es una herramienta de código cerrado, no hay manera de verificar esta alegación, pero muchas personas creen que es cierta. Skype también ofrece el servicio de mensajería instantánea.

- **Software gratuito (freeware)** – Incluye software sin costo pero que está sujeto a restricciones legales o técnicas que le impiden al usuario acceder al código fuente utilizado para crearlo.
- **Software Libre y de Código Abierto (FOSS)** – Esta familia de software está disponible gratuitamente y no tiene restricciones legales que impidan a un usuario probarlo, compartirlo o modificarlo.
- **Software malicioso (malware)** – Término general para referirse a cualquier software malicioso, entre ellos *virus, software espía (spyware), troyanos,* y otras amenazas similares.
- **Software propietario** – Es el opuesto al software libre y de código abierto (FOSS). Estas aplicaciones son normalmente comerciales, pero también pueden ser *software libre* con requisitos de licencia restrictivos.
- **Spybot** – Herramienta de software libre que combate el software malicioso (malware), por ello escanea, elimina y ayuda a proteger tu computadora de cualquier software espía (spyware).
- **Tarjeta SIM** – Tarjeta pequeña y desmontable que puede ser insertada en un teléfono móvil con el fin de proporcionar servicio con una compañía de telefonía móvil en particular. Las tarjetas SIM también pueden almacenar números telefónicos y mensajes de texto.
- **Thunderbird** – Programa de correo electrónico de software libre y de código abierto con varias características de seguridad, entre ellas la admisión del complemento de cifrado *Enigmail*.
- **Tor** – Herramienta de anonimato que te permite evadir la censura en Internet y ocultar las páginas web y servicios de Internet que visitas de cualquiera que pudiera estar vigilando tu conexión a Internet. Al mismo tiempo esta herramienta oculta tu ubicación a aquellos sitios web a los que ingresas.
- **TrueCrypt** – Herramienta de cifrado de archivos de software libre y código abierto que te permite almacenar información sensible de manera segura.
- **Undelete Plus** – Herramienta de software libre que a veces puede restituir la información que pudieras haber borrado de manera accidental.
- **VauletSuite 2 Go** - Programa de software gratuito para cifrado de correo electrónico.
- **Voz sobre Protocolo de Internet (VoIP)** – Tecnología que te permite utilizar Internet para comunicaciones por voz con otros usuarios de *Voz sobre Protocolo de Internet* y teléfonos.
- **Your-Freedom** – Herramienta de evasión de software libre que te permite evadir filtros en la Internet por medio de una conexión a un proxy privado. Si Your-Freedom esta configurado adecuadamente, tu conexión a estos proxies será cifrada con el fin de proteger la privacidad de tus comunicaciones.